

**CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS**  
**PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO**  
**CLAUDIO JUNIOR NASCIMENTO DA SILVA**

**GOVERNANÇA E ALINHAMENTO ESTRATÉGICO DE TIC E NEGÓCIO NO**  
**ÂMBITO DAS EMPRESAS SERGIPANAS: proposta de melhorias na Metodologia PETIC**  
**a partir da gestão de riscos e da comunicação e transparência de TIC**

**SÃO CRISTÓVAO**  
**2017**

**CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS**  
**PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO**  
**CLAUDIO JUNIOR NASCIMENTO DA SILVA**

**GOVERNANÇA E ALINHAMENTO ESTRATÉGICO DE TIC E NEGÓCIO NO**  
**ÂMBITO DAS EMPRESAS SERGIPANAS: proposta de melhorias na Metodologia PETIC**  
**a partir da gestão de riscos e da comunicação e transparência de TIC**

Dissertação do Programa de Pós-Graduação em Ciência da Computação (PROCC) da Universidade Federal de Sergipe (UFS) como parte de requisito para obtenção do título de Mestre em Ciência da Computação.

**Orientador:** Prof. Dr. Rogério Patrício Chagas do Nascimento.

**Coorientador:** Prof. Dr. Methanias Colaço Rodrigues Júnior.

**SÃO CRISTÓVAO**

**2017**

**FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL  
UNIVERSIDADE FEDERAL DE SERGIPE**

S586g Silva, Claudio Junior Nascimento da  
Governança e alinhamento estratégico de TIC e negócio no âmbito das empresas sergipanas : proposta de melhorias na metodologia PETIC a partir da gestão de riscos e da comunicação e transparência de TIC / Claudio Junior Nascimento da Silva ; orientador Methanias Colaço Rodrigues Júnior. – São Cristóvão, 2017.  
119 f. : il.

Dissertação (mestrado em Ciências da computação)–  
Universidade Federal de Sergipe, 2017.

1. Ciência da computação.. 2. Planejamento estratégico. 3. Gerenciamento de risco. 4. Tecnologia da informação. 5. Comunicação da tecnologia. I. Rodrigues Júnior, Methanias Colaço. II. Título.

CDU: 004:005

**GOVERNANÇA E ALINHAMENTO ESTRATÉGICO DE TIC E NEGÓCIO NO  
ÂMBITO DAS EMPRESAS SERGIPANAS: proposta de melhorias na Metodologia PETIC  
a partir da gestão de riscos e da comunicação e transparência de TIC**

**BANCA EXAMINADORA**

Este exemplar corresponde à redação final da  
Dissertação de Mestrado, sendo o Exame de Defesa  
do mestrando **CLAUDIO JUNIOR  
NASCIMENTO DA SILVA**, para ser aprovada pela  
Banca Examinadora.

São Cristóvão - SE, 31 de maio de 2017.

---

Profº Drº Rogério Patrício Chagas do Nascimento  
Orientador

---

Profº Drº Methanias Colaço Rodrigues Júnior  
Coorientador

---

Profº Drº Jefferson David Araújo Sales  
Membro Externo

## DEDICATÓRIA

---

Dedico este trabalho ao meu pai, Claudio Vitorio da Silva (*in memoriam*), pela referência e exemplo de vida; à minha mãe Railda, sempre presente; e à minha amada esposa, Patrícia, que desde o início me incentivou e me apoiou.

## AGRADECIMENTOS

---

Ao Grande Arquiteto do Universo, responsável pela criação e razão da existência de tudo, agradeço pela oportunidade de viver e sentir sua presença em todas as coisas.

Ontem, hoje e sempre ao meu pai, exemplo de homem, que me ensinou que a educação e o conhecimento são o caminho para o crescimento pessoal. À minha mãe, referência de mulher, que cuidou de mim, me educou e ensinou as primeiras letras. À minha madrinha e tia, pelo apoio, força e confiança.

Gratidão e agradecimentos à minha amada esposa Patrícia, que jamais deixou de me apoiar e incentivar, auxiliando-me e dando-me forças para seguir em frente.

Um agradecimento especial a Rogério e a Methanias, pela orientação, paciência e dedicação. Que os bons ventos os levem por bons caminhos.

Muito obrigado aos colegas do Mestrado, em especial aos “*Minions* do Rogério”.

Retornando ao passado, reconheço e agradeço a Tia Cici (*in memoriam*) e assim o fazendo, agradeço aos verdadeiros MESTRES que me prepararam para sempre buscar a educação.

Meus agradecimentos a Companhia Industrial Têxtil, mais que um local de trabalho, um espaço onde é possível colocar em prática o aprendizado adquirido.

A minha família e a todos aqueles que fisicamente não estão entre nós, como Tia Gery, Tio Gilson, Vovó Hilda e Tio Zé Gringo, mas que onde se encontram estão felizes por mais essa vitória.

Também um agradecimento especial aos meus irmãos e irmãs de fé, que em corrente de união muito me ajudaram, emanando forças e vibrações para superar todas as dificuldades.

Obrigado a todos aqueles que, de alguma forma, contribuíram para o meu crescimento pessoal e para a realização deste trabalho.

## LISTA DE FIGURAS

---

Figura 1- Etapas para elaboração da pesquisa .....	25
Figura 2- Modelo de Henderson e Venkatraman .....	31
Figura 3- Governança de TIC.....	34
Figura 4- Componentes da Metodologia PETIC .....	35
Figura 5 - Artefato PETIC .....	37
Figura 6 - Etapas detalhadas do PE .....	38
Figura 7 - Matriz de prioridade (probabilidade x impacto) .....	40
Figura 8 - Fluxo da elaboração da proposta da gestão de riscos de TIC .....	75
Figura 9- Mapa dos riscos de TIC .....	78
Figura 10 - Fluxo da elaboração da proposta da gestão de comunicação e transparência de TIC .....	80
Figura 11 - Proposta de alteração do <i>workflow</i> PETIC .....	83
Figura 12 - Proposta de novos componentes na Metodologia PETIC.....	84

## LISTA DE GRÁFICOS

---

Gráfico 1- Importância do alinhamento estratégico entre TIC e negócio.....	56
Gráfico 2- Tamanho das organizações.....	57
Gráfico 3- Práticas de governança de TIC .....	60
Gráfico 4- Governança na organização: definição dos papéis e gestão de riscos .....	63
Gráfico 5- Governança na organização: processos e informatização.....	65
Gráfico 6- Periodicidade do planejamento estratégico na organização.....	68
Gráfico 7- PE da organização, PE de TIC e alinhamento estratégico .....	68
Gráfico 8- Consciência da alta direção sobre a importância do alinhamento estratégico.....	70
Gráfico 9- Gráfico de impacto x custos dos riscos de TIC.....	78



## LISTA DE TABELAS

---

Tabela 1- Função dos entrevistados.....	55
Tabela 2- Certificações dos entrevistados.....	55
Tabela 3- Ramo de atuação/segmento da organização.....	57
Tabela 4- Serviços sob a responsabilidade da gestão de TIC.....	58
Tabela 5- Ferramentas, <i>softwares</i> e sistemas de apoio.....	59
Tabela 6- Práticas de Governança de TIC utilizadas .....	61
Tabela 7- Práticas de governança de TIC x tamanho da organização .....	61
Tabela 8- Benefícios da utilização de práticas de governança de TIC.....	62
Tabela 9- Motivos para não adotar a gestão de riscos.....	64
Tabela 10 - Riscos integrantes de um plano de gestão de riscos de TIC.....	64
Tabela 11- Processo de <i>software</i> nas organizações .....	66
Tabela 12- Abordagens de engenharia de <i>software</i> .....	67
Tabela 13- Planejamento estratégico de TIC.....	69
Tabela 14 - Comunicação e transparência de TIC.....	70
Tabela 15- Vantagens do alinhamento do PE da organização e o PE de TIC .....	71
Tabela 16- Dificuldades para implantação do PE de TIC .....	71
Tabela 17 - Utilização de processos do catálogo de processos de TIC .....	89
Tabela 18 - Relação de novos processos de TIC utilizados.....	89
Tabela 19 - Indicadores de avaliação - catálogo dos riscos de TIC .....	92

## LISTA DE QUADROS

---

Quadro 1 - Práticas de governança de TIC.....	33
Quadro 2- Comparativo das abordagens da gestão de riscos.....	45
Quadro 3- Organização do questionário .....	52
Quadro 4 - Atributos do catálogo dos riscos de TIC.....	76
Quadro 5 - Exemplo do catálogo dos riscos de TIC .....	77
Quadro 6 - Atributos do plano de comunicação e transparência de TIC.....	81
Quadro 7 - Exemplo do plano de comunicação e transparência de TIC .....	82
Quadro 8 - Indicadores de medição do estudo de caso .....	87
Quadro 9 - Análise do catálogo de riscos.....	92
Quadro 10 – Análise do catálogo de comunicação e transparência de TIC.....	93
Quadro 11 - Resultado da avaliação qualitativa das propostas de melhorias na Metodologia PETIC .....	94

## LISTA DE ABREVIATURAS E SIGLAS

---

<b>BSC</b>	<i>Balanced Score Card</i>
<b>BI</b>	<i>Business Intelligence</i>
<b>CIO</b>	<i>Chiefs Information Officer</i>
<b>CIO-SE</b>	<i>Associação dos Gestores de Tecnologia da Informação do Estado de Sergipe</i>
<b>CMMI</b>	<i>Capability Maturity Model Integration</i>
<b>CN</b>	<i>Continuidade dos Negócios</i>
<b>COBIT</b>	<i>Control Objectives for Information and Related Technology</i>
<b>CPD</b>	<i>Centro de Processamento de Dados</i>
<b>DCOMP</b>	<i>Departamento de Computação</i>
<b>EAP</b>	<i>Estrutura Analítica do Projeto</i>
<b>ERP</b>	<i>Enterprise Resource Planning (Sistema de Gestão Integrada)</i>
<b>GQM</b>	<i>Goal Question Metric</i>
<b>ISACA</b>	<i>Information System Audit and Control Association (ISACA)</i>
<b>ITIL</b>	<i>Information Technology Infrastructure Library</i>
<b>PE</b>	<i>Planejamento Estratégico</i>
<b>PE de TIC</b>	<i>Planejamento Estratégico de Tecnologia da Informação e Comunicação</i>
<b>PMBOK</b>	<i>Project Management Body of Knowledge</i>
<b>PME</b>	<i>Pequenas e Médias Empresas</i>
<b>SGSI</b>	<i>Sistema de Gestão da Segurança da Informação</i>
<b>SI</b>	<i>Segurança da Informação</i>
<b>TCU</b>	<i>Tribunal de Contas da União</i>
<b>TIC</b>	<i>Tecnologia da Informação e Comunicação</i>
<b>UFS</b>	<i>Universidade Federal de Sergipe</i>

<b>1</b>	<b>INTRODUÇÃO.....</b>	<b>17</b>
1.1	Contextualização.....	17
1.2	Problemática e Motivação .....	18
1.3	Objetivos .....	22
1.4	Contribuições Esperadas .....	23
1.5	Metodologia de Pesquisa.....	23
1.5.1.	<i>Survey</i> .....	26
1.5.2.	Estudo de Caso .....	26
1.6	Organização da Dissertação.....	27
<b>2</b>	<b>REFERENCIAL TEÓRICO.....</b>	<b>28</b>
2.1	Planejamento Estratégico .....	28
2.2	Planejamento Estratégico de Tecnologia da Informação e Comunicação .....	29
2.3	Alinhamento Estratégico entre TIC e Negócio .....	30
2.4	Governança de TIC.....	32
2.5	Metodologia PETIC.....	34
2.5.1.	Os Componentes da Metodologia PETIC .....	35
2.5.2.	Catálogo de processos de TIC .....	35
2.5.3.	Repositório de Ações .....	36
2.5.4.	Catálogo de Ferramentas e Técnicas.....	36
2.5.5.	O Artefato PETIC .....	36
2.5.6.	O <i>Workflow</i> da Metodologia PETIC.....	38
2.6	Gestão de Riscos de TIC .....	38
2.6.1.	Abordagem PMBOK .....	39
2.6.2.	Abordagem ITIL.....	41
2.6.3.	Abordagem COBIT.....	42
2.6.4.	Abordagem CMMI .....	44
2.6.5.	Abordagem ISO 27005 .....	44
2.6.6.	Comparativo das Abordagens.....	45
2.7	Gestão da Comunicação e Transparência de TIC .....	46
2.7.1.	Abordagem PMBOK .....	46
2.7.2.	Abordagem ITIL.....	47
2.7.3.	Abordagem COBIT.....	48
2.7.4.	Abordagem CMMI .....	49
<b>3</b>	<b><i>SURVEY</i>: GOVERNANÇA E ALINHAMENTO ESTRATÉGICO DE TIC E NEGÓCIO .....</b>	<b>50</b>
3.1	Planejamento .....	50

3.1.1.	Seleção de Participantes e Tamanho da Amostra.....	50
3.1.2.	Metodologia .....	51
3.1.3.	Organização do Questionário .....	52
3.1.4.	Instrumentação .....	53
3.2	Operação .....	53
3.2.1.	Aplicação .....	53
3.2.2.	Coleta e Validação de Dados .....	54
3.3	Interpretação dos Resultados .....	54
3.3.1.	Resultados Brutos .....	54
3.3.1.1.	Identificação do Entrevistado .....	54
3.3.1.2.	Identificação da Organização .....	56
3.3.1.3.	Estrutura de TIC .....	58
3.3.1.4.	Governança de TIC.....	59
3.3.1.5.	Planejamento e Alinhamento Estratégico.....	67
3.3.2.	Ameaças à Validade.....	72
3.4	Considerações Finais do Capítulo.....	72
<b>4</b>	<b>PROPOSTA DE MELHORIAS NA METODOLOGIA PETIC .....</b>	<b>74</b>
4.1	Gestão de Riscos de TIC .....	74
4.1.1.	Elaboração da Proposta da Gestão de Riscos de TIC.....	75
4.1.2.	Catálogo dos Riscos de TIC .....	76
4.1.3.	Gráficos para Análise dos Riscos de TIC.....	77
4.1.4.	Plano de Respostas aos Riscos de TIC.....	79
4.2	Gestão da Comunicação e Transparência de TIC .....	79
4.2.1.	Elaboração da Proposta do Plano de Comunicação e Transparência de TIC.....	80
4.2.2.	Plano de Comunicação e Transparência de TIC .....	81
4.3	Proposta de Alteração no Workflow da Metodologia PETIC.....	82
4.4	Considerações Finais do Capítulo.....	84
<b>5</b>	<b>ESTUDO DE CASO.....</b>	<b>86</b>
5.1	Etapas e Diretrizes para o Estudo de Caso .....	86
5.1.1.	Projeto do Estudo de Caso.....	86
5.1.2.	Preparação para a Coleta de Dados .....	87
5.1.3.	Coleta de Evidências.....	87
5.1.3.1.	Estudo de Caso Companhia Têxtil.....	88
5.1.4.	Forma de Coleta das Evidências.....	91
5.1.5.	Análise dos Dados Coletados .....	91
5.2	Considerações Finais do Capítulo.....	95

<b>6</b>	<b>CONSIDERAÇÕES FINAIS .....</b>	<b>96</b>
6.1	Principais Contribuições .....	97
6.2	Consolidação e Divulgação dos Resultados .....	98
6.3	Limitações e Dificuldades da Pesquisa .....	98
6.4	Trabalhos Futuros .....	99
	<b>REFERÊNCIAS .....</b>	<b>100</b>
	<b>APENDICES .....</b>	<b>104</b>
	<b>APENDICE A – CATÁLOGO DE RISCOS DE TIC .....</b>	<b>105</b>
	<b>APENDICE B – PLANO DE RESPOSTA AOS RISCOS DE TIC .....</b>	<b>109</b>
	<b>APENDICE C – PLANO DE COMUNICAÇÃO E TRANSPARÊNCIA DE TIC .....</b>	<b>118</b>
	<b>APENDICE D – CRITÉRIOS DE PRIORIZAÇÃO DOS PROCESSOS DE TIC .....</b>	<b>119</b>

Em um mercado cada vez mais competitivo os recursos de Tecnologia da Informação e Comunicação (TIC) são essenciais e estratégicos nas organizações. Atualmente, o uso das TICs é uma questão de sobrevivência do negócio. Da mesma forma que as organizações e o mercado estão em constantes mudanças, as TICs estão em constante evolução, não sendo mais concebível tratá-las apenas como recursos de apoio, mas também como um recurso estratégico, com riscos para o negócio e sendo conhecido por todos. Consequentemente, o emprego dos recursos tecnológicos deve estar alinhado com os objetivos do negócio. Faz-se necessário, então, identificar como as organizações estão promovendo o alinhamento das estratégias de TIC com as estratégias do negócio e como estão sendo tratadas as questões dos riscos e da comunicação e transparência de TIC. O presente trabalho investigou, após a aplicação de um questionário eletrônico (*survey*) aos *Chiefs Information Officer* sergipanos, como as práticas de governança de TIC são adotadas pelas empresas e como se encontram o planejamento e o alinhamento estratégico entre TIC e negócio. Como resultado, observou-se uma carência das organizações na gestão de riscos, dos processos de comunicação e do alinhamento estratégico entre TIC e negócio, bem como se constatou que as principais práticas de governança da TIC utilizadas foram Planejamento Estratégico de TIC próprio ou customizado, ITIL, PMBOK e BSC. Além das práticas de governança de TIC citadas, existem outras metodologias e *frameworks* que propõem a gestão eficiente dos objetivos de TIC, alinhados com a estratégia organização, dentre elas a Metodologia PETIC, desenvolvida pela Universidade Federal de Sergipe. Neste cenário, são propostas melhorias na Metodologia PETIC, incorporando ao seu escopo a gestão de riscos e gestão da comunicação e transparência de TIC, possibilitando uma avaliação de TIC eficiente e alinhada com os objetivos estratégicos do negócio. Para evidenciar a suposição apresentada que *a inclusão da gestão de riscos e de comunicação e transparência na Metodologia PETIC permitem a elaboração de um PE de TIC mais alinhado com os objetivos do negócio* um estudo de caso foi aplicado em uma empresa sergipana e, por meio de análises qualitativas e quantitativas das métricas previamente definidas, constatou-se o aprimoramento na elaboração do planejamento estratégico de TIC e na gestão dos riscos e da comunicação e transparência.

**Palavras-chave:** Governança de TIC. Melhores Práticas. Planejamento Estratégico. Alinhamento Estratégico. Riscos. Comunicação e Transparência. PETIC.

## ABSTRACT

---

In an increasingly competitive market, Information and Communication Technology (ICT) resources are essential and strategic in organizations. Today, the use of ICTs is a matter of business survival. In the same way that organizations and the market are constantly changing, ICTs are constantly evolving, and it is no longer conceivable to treat them only as support resources, but also as a strategic resource, with risks to the business and being known by all. Consequently, the use of technological resources must be in line with business objectives. It is therefore necessary to identify how organizations are promoting the alignment of ICT strategies with business strategies and how issues of risk and ICT communication and transparency are being addressed. The present work investigated, after the application of an electronic questionnaire (survey) to the Chief Information Officers sergipanos, how the ICT governance practices are adopted by the companies and how they are the planning and the strategic alignment between ICT and business. As a result, there was a lack of organizations in risk management, communication processes and strategic alignment between ICT and business, as well as found that the main ICT governance practices used were own or customized ICT Strategic Planning, ITIL, PMBOK and BSC. In addition to the ICT governance practices cited, there are other methodologies and frameworks that propose efficient management of ICT objectives, aligned with the organizational strategy, among them the PETIC Methodology, developed by the Federal University of Sergipe. In this scenario, improvements are proposed in the PETIC Methodology, incorporating in its scope risk management and communication management and ICT transparency, enabling an ICT assessment that is efficient and in line with the strategic business objectives. In order to demonstrate the supposition that the inclusion of risk management and communication and transparency in the PETIC Methodology allows for the elaboration of an ICT PE more aligned with the business objectives, a case study was applied in a Sergipe company and, through Qualitative and quantitative analyzes of the metrics previously defined, the improvement in the elaboration of the strategic planning of ICT and in the management of risks and communication and transparency.

**Keywords:** ICT Governance. Best Practices. Strategic planning. Strategic Alignment. Scratches. Communication and Transparency. PETIC.



## 1 INTRODUÇÃO

---

Este capítulo pretende realizar uma breve contextualização relacionada ao tema da pesquisa, motivação, problemática, questões, objetivos e suposição que se pretende evidenciar. Além disso, são descritas as contribuições que se esperam alcançar ao final do trabalho e a metodologia de pesquisa direcionadora do trabalho. Por fim, apresenta-se a organização da dissertação.

### 1.1 CONTEXTUALIZAÇÃO

A Tecnologia da Informação e Comunicação (TIC) fornece serviços necessários e importantes para o negócio, tais como planejar, gerenciar os serviços, armazenar e proteger dados, tornando-se parte vital em muitas atividades organizacionais. Por meio do alinhamento entre o Planejamento Estratégico (PE) de negócio e o Planejamento Estratégico de TIC (PE de TIC) possibilita-se o alcance das metas da organização. (ATESE; TANRIÖVER, 2014).

Além disso, com tantas atividades de TIC acontecendo fora dos departamentos de TIC, as organizações encontrarão questões críticas envolvendo privacidade, segurança e riscos. Isso criará novos desafios importantes para as áreas de tecnologia e para os líderes de segurança (GARTNER, 2017).

Para garantir que a empresa não tenha perdas financeiras, desgastes nas relações ou que aumente sua exposição ao risco é necessário que a organização se preocupe com a TIC. Quaisquer decisões estratégicas tomadas pela organização podem provocar reações imediatas nas áreas de TIC, tais como: segurança da informação, *hardware*, telecomunicações, engenharia de *software*, engenharia de requisitos, *business intelligence*, processos (AUDY; BRODBECK, 2003).

Não apenas na área TIC, mas em uma organização como um todo, insucessos nos resultados operacionais e financeiros, performances indesejadas distantes de um planejamento justo, podem resultar em demissões, mudanças de rotas e críticas ao trabalho desenvolvido. Entretanto, o sucesso é pautado muito mais na preparação e no planejamento do que simplesmente no atingimento das metas.

Segundo Kaspersky (2017) o investimento em segurança da informação é prioridade para os bancos e instituições financeiras. Ao sofrer ataques em sua própria infraestrutura e na de clientes, os bancos de varejo gastam três vezes mais em segurança de TIC que instituições de

outras áreas com porte semelhante. Além disso, 64% dos bancos admitem que investiram para melhorar sua segurança de TIC, independente do retorno do investimento, de modo a atender às demandas crescentes das agências regulatórias do governo, da alta direção e até mesmo de seus clientes.

Assim como o mundo, as TIC aceleram rapidamente para maior complexidade em todos os aspectos das nossas vidas. Entender e gerenciar os riscos será cada vez mais desafiador. Ainda que imprescindível, a gestão de riscos precisa ser complementada com "redes de proteção" para assegurar que os negócios sejam resilientes a quaisquer riscos que se transformem em ameaças reais. A Continuidade de Negócios (CN) é conhecida aliada neste processo (CARISSIMI, 2017).

As organizações podem ser surpreendidas a qualquer momento com um novo e avançado ataque, ou a concretização de um risco considerado baixo e aceitável. A lógica é negligenciar eventos de alto impacto, se a probabilidade é baixíssima, pois os recursos da empresa precisam ser otimizados. Até que ponto faz sentido proteger-se de eventos que nunca acontecem? Neste sentido, uma governança adequada dos riscos é peça fundamental dentro da organização (CARISSIMI, 2017).

Evidencia-se, dessa forma, o papel central e importante da TIC e do gestor, não só no gerenciamento das atividades técnicas pertinentes ao setor, como também as atividades de planejamento e parceria com o negócio da empresa. É notório que as responsabilidades são ampliadas e, para tanto, cabe ao gestor de TIC se municiar de mecanismos e ferramentas que possibilitem uma gestão proativa, antecipando-se a problemas, evitando e mitigando riscos e analisando dados que lhe permitam a tomada de decisão com maior segurança permitindo assim a garantia de disponibilidade dos serviços e recursos de TIC. O controle e a métrica serão os conceitos fundamentais para que se obtenha êxito na gestão, afirma Rezende (2011).

## **1.2 PROBLEMÁTICA E MOTIVAÇÃO**

A tecnologia está em constante mudança e a complexidade aumenta com esta. Atualmente a agilidade representa um desafio para muitos. Por isso a TIC desempenha um papel proeminente na agilidade empresarial, permitindo rápida e contínua inovação em produtos, serviços, formas de fornecimento e gestão (REZENDE, 2011; TEXTOR *et al.*, 2015).

Os recursos de TIC, se utilizados devidamente, permitem um melhor desempenho da organização, do negócio, das ações a serem realizadas para o aumento da competitividade e atingimento de metas, além da gestão dos bens físicos, financeiros e dos recursos humanos com

maior rapidez e precisão (LIMA, 2007). Nesse contexto, o alinhamento entre as estratégias de TIC e de negócio passa a se tornar uma estratégica ferramenta de gestão que possibilita a criação de diferenciais competitivos (LAURINDO, 2008).

Para a obtenção de sucesso na adoção de um PE de TIC, este deve estar alinhado à estratégia organizacional e pautado em uma governança de TIC eficaz. Sem o apoio de ferramentas adequadas, o gestor apresenta sérias limitações que podem impactar significativamente no resultado da implantação de uma metodologia ligada à Governança de TIC (PALMEIRA *et al.*, 2012).

Visando o alinhamento estratégico dos planos de negócio e de TIC, aplicam-se modelos de governança de TIC utilizando algumas das melhores práticas de gestão, dentre elas (AZEVEDO, 2013):

- PE de TIC;
- *Control Objectives for Information and Related Technology* (COBIT);
- *Information Technology Infrastructure Library* (ITIL);
- Capability Maturity Model Integration (CMMI);
- *Project Management Body of Knowledge* (PMBOK);
- Gestão da Segurança da Informação (ISO/IEC 27001 ou 27002);
- *Balanced Score Card* (BSC).

Outro modelo de apoio à governança de TIC é a Metodologia PETIC, concebida dentro do Grupo de Pesquisa em Engenharia de *Software* da Universidade Federal de Sergipe (UFS). A PETIC representa uma metodologia para elaboração do PE de TIC e aborda as seis grandes áreas de Sistemas de Informação (SI), a saber: dados, *software*, *hardware*, telecomunicações, pessoas e Governança de TIC (PALMEIRA, 2012).

Partindo desse pressuposto, surgiu a primeira questão que motiva a presente pesquisa: *quais e como são utilizadas as práticas de governança de TIC adotadas pelas empresas do estado de Sergipe que visam o alinhamento estratégico entre TIC e negócio?*

A primeira questão foi investigada aplicando um questionário eletrônico (*survey*) aos *Chiefs Information Officer* (CIO) sergipanos, sobre como as práticas de governança de TIC são adotadas pelas empresas e como se encontram o planejamento e o alinhamento estratégico entre TIC e negócio, cujos resultados são descritos nas seções seguintes.

Foram definidas algumas variáveis que subsidiassem a busca da resposta para a primeira grande questão, entre elas estão: frequências, perfazendo a lista (número) de respostas por práticas de governança de TIC utilizadas nas empresas; o percentual (frequência) de empresas cuja alta direção tem conhecimento sobre a importância e a necessidade do alinhamento

estratégico entre TIC e negócio; o percentual (frequência) de empresas que adotam formalmente o planejamento estratégico da organização, o planejamento estratégico de TIC e o alinhamento estratégico entre TIC e negócio; a lista (número) das práticas de governança TIC utilizadas pelas empresas sergipanas e o número de empresas por prática utilizada.

Segundo ISACA(2015), o alinhamento estratégico das ações da TIC com as do negócio, com o intuito de alcançar os objetivos corporativos, é obtido por meio da eficiência e eficácia da comunicação e transparência da organização para com as pessoas.

Para o Gartner (2017) é necessário criar organizações resilientes, que continuem alcançando seus objetivos corporativos diante do número crescente de ameaças na segurança da informação. Faz-se necessário não proteger apenas a infraestrutura, mas também dar suporte aos resultados do negócio, revisando ou implementando estratégias de segurança e de gestão de riscos para atingirem os resultados desejados do negócio. Nesse sentido, e com vistas a resolver falhas, surgiu a segunda questão motivadora da pesquisa: *como criar mecanismos que possibilitem uma gestão efetiva dos riscos e gestão da comunicação e transparência de TIC?*

Para responder a esta segunda questão serão propostas melhorias na Metodologia PETIC para incorporar em seu escopo a gestão de riscos de TIC e da comunicação e transparência de TIC. Ela foi escolhida como objeto de estudo por se tratar de uma metodologia desenvolvida internamente na UFS; por necessitar de constante aprimoramento para atender as necessidades das organizações, devido à facilidade na implementação de novos procedimentos e processos, por não ser embarcada, ou seja, restrita às alterações; e, pelo fácil acesso aos responsáveis por sua manutenção.

Para subsidiar as respostas da segunda questão, foram definidas as seguintes variáveis: número total de riscos do catálogo proposto; número de riscos do catálogo da organização; número de informações do plano de comunicação e transparência proposto; número de informações do plano de comunicação e transparência da organização e análise dos questionários de avaliação.

A partir destas indagações, um conjunto de questões subjacentes é colocado para discussão:

- *As empresas sergipanas utilizam práticas de governança de TIC?*
- *A alta direção das empresas sergipanas tem conhecimento da importância e da necessidade do alinhamento estratégico entre TIC e negócio?*
- *As empresas sergipanas adotam formalmente o planejamento estratégico da organização, o planejamento estratégico de TIC e o alinhamento entre TIC e negócio?*

- *As melhorias propostas na Metodologia PETIC promovem uma gestão mais eficiente dos riscos e da comunicação e transparência de TIC?*

Segundo Martins (2002), o problema de pesquisa pode surgir de circunstâncias pessoais ou profissionais, da experiência científica, da leitura de grandes obras e revistas especializadas ou mesmo como sugestão de uma personalidade superior. Ressalta-se, que o problema de pesquisa é formulado, elaborado e construído pelo pesquisador para permitir-lhe a investigação.

Para Vergara (2000), o problema é uma questão não resolvida, é algo para o qual se vai buscar resposta, via pesquisa. Uma questão não resolvida pode estar referida a alguma lacuna epistemológica ou metodológica percebida, a alguma dúvida quanto à sustentação de uma afirmação geralmente aceita, a alguma necessidade de pôr à prova uma suposição, a interesses práticos, à vontade de compreender e explicar uma situação do cotidiano ou outras situações.

Identificado o problema, faz-se necessária a elaboração de uma suposição passível de investigação dentro da proposta desta dissertação. A suposição em questão é: *a inclusão da gestão de riscos e de comunicação e transparência na Metodologia PETIC permitem a elaboração de um PE de TIC mais alinhado com os objetivos do negócio*. Para evidenciar esta suposição, um estudo de caso foi aplicado em uma empresa sergipana e, por meio de métricas previamente definidas, análises quantitativas e qualitativas foram realizadas.

Não foram encontrados *surveys* científicos com o mesmo objeto de pesquisa desta dissertação inclusive tratando da caracterização dos processos de negócio e da gestão de riscos e de comunicação e transparência de TIC no Brasil em relação às práticas de governança de TIC. Este fato aumenta a importância dos dados aqui apresentados. Além disso, esta dissertação difere de grande parte dos *surveys* apresentados na área de computação, pois engloba a avaliação de CIOs, ou seja, gestores que possuem o poder de decisão ou influenciam na decisão acerca da aplicação de recursos de TIC. Dentre os trabalhos encontrados, alguns foram destacados no intuito de situar a presente pesquisa, mesmo que moderadamente relacionados.

Rogério e Amboni (2007) apresentam os aspectos que podem contribuir para o alinhamento do planejamento de negócio com o planejamento dos CIOs das empresas de Santa Catarina. Os aspectos estudados (formalização do PE, formalização do PE de TIC, mapeamento dos processos, gestão da infraestrutura de TIC, gestão de riscos, utilização de práticas de governança de TIC, entre outros) promovem o alinhamento de forma contínua entre os processos das organizações que tem suporte da TIC como papel importante no processo organizacional.

Um estudo quantitativo foi realizado por Tarouco e Graeml (2011) com a finalidade de compreender e caracterizar a adoção de práticas de Governança de TIC a partir da visão dos

executivos. Os autores concluíram que a governança de TIC está ligada diretamente às iniciativas relacionadas ao aumento de controle e qualidade dos serviços de TIC à empresa.

Na pesquisa apresentada por Jaana *et al.* (2012) foi avaliada a aplicação de práticas de TIC para agregar valor no negócio e aumentar o retorno do investimento em TIC. Outros pontos avaliados foram a flexibilidade e a capacidade que a TIC possui nos resultados e nas mudanças que ocorrem na administração pós-implementação.

Estes trabalhos instigam a investigação de como empresas sergipanas estão tratando o alinhamento do PE com o PE de TIC, a gestão de riscos e a gestão da comunicação e transparência de TIC e se as práticas e processos existentes estão sendo utilizados adequadamente. Além disso, estimulam a criação da suposição sobre a necessidade de adoção de novas práticas para este fim.

### 1.3 OBJETIVOS

O objetivo principal do presente trabalho é analisar a utilização da governança de TIC no alinhamento estratégico entre TIC e negócio no âmbito das empresas sergipanas e propor melhorias na Metodologia PETIC, incorporando ao seu escopo a gestão de riscos e da comunicação e transparência de TIC.

Como objetivos específicos, são propostos:

- Aplicar um *survey* cujo público-alvo seja os CIOs das empresas sergipanas, com o intuito de identificar o panorama de adoção de práticas de governança de TIC nas empresas;
- Propor, com base nas práticas de Governança de TIC, a inclusão do catálogo de riscos e do plano de respostas aos riscos na Metodologia PETIC;
- Sugerir a incorporação do plano de comunicação e transparência de TIC na Metodologia PETIC;
- Propor alterações no *workflow* da Metodologia PETIC, adequando-o à gestão de riscos e gestão da comunicação e transparência de TIC;
- Realizar um estudo de caso para avaliar as propostas de melhorias apresentadas.

## 1.4 CONTRIBUIÇÕES ESPERADAS

Os recursos de TIC são parte integrante do negócio, sendo afetadas por ele, bem como o afetando significativamente. Não podem ser considerados isoladamente, mas sim conforme sua interação com os objetivos e estratégias propostas.

Ao realizar esse estudo sobre a utilização de práticas de governança de TIC como ferramenta para a consecução do alinhamento dos objetivos de TIC com o negócio e ao sugerir a incorporação da gestão de riscos e da comunicação e transparência na Metodologia PETIC, espera-se como contribuição:

- Ajudar na promoção da pesquisa científica no universo da indústria, aproximando-a do meio acadêmico;
- Realizar um estudo pioneiro que revele as características da utilização de práticas de governança de TIC no estado de Sergipe;
- Disponibilizar estudo preliminar que possibilite o desenvolvimento de novas pesquisas no âmbito das práticas de governança, planejamento e alinhamento estratégico de TIC;
- Dispor de um modelo simples que permita a gestão de riscos e gestão da comunicação e transparência de TIC nas organizações;
- Contribuir com o aperfeiçoamento e a evolução da Metodologia PETIC ampliando seu escopo na disponibilização de processos de gestão de riscos e gestão da comunicação e transparência.

## 1.5 METODOLOGIA DE PESQUISA

Um método é um conjunto de processos pelos quais se torna possível conhecer uma determinada realidade, produzir determinado objeto ou desenvolver certos procedimentos ou comportamentos. O método científico caracteriza-se pela escolha de procedimentos sistemáticos para descrição e explicação de uma determinada situação sob estudo e sua escolha deve estar baseada em dois critérios básicos: a natureza do objeto ao qual se aplica e o objetivo que se tem em vista no estudo (MAY, 2004); (YIN, 2001); (OLIVEIRA, 1997); (FACHIN, 2001).

O enquadramento metodológico deste trabalho está alinhado às seguintes modalidades de pesquisa científica:

- *Quanto à natureza de pesquisa:* **Pesquisa Aplicada**. Segundo Gil (1999), a pesquisa aplicada tem como característica fundamental o interesse na aplicação,

utilização e consequências práticas dos conhecimentos. Sua preocupação está menos voltada para o desenvolvimento de teorias de valor universal que para a aplicação imediata numa realidade circunstancial;

- *Quanto à abordagem do problema:* **Pesquisa Quantitativa e Qualitativa**. A pesquisa quantitativa se centra na objetividade. Considera que a realidade só pode ser compreendida com base na análise de dados brutos, recolhidos como auxílio de instrumentos padronizados e neutros. Recorre à linguagem matemática para descrever as causas de um fenômeno, as relações entre variáveis, etc. A pesquisa qualitativa trabalha com o universo de significados, motivos, aspirações, crenças, valores e atitudes, o que corresponde a um espaço mais profundo das relações, dos processos e dos fenômenos que não podem ser reduzidos à operacionalização de variáveis. (GERHARDT; SILVEIRA, 2009);
- *Quanto aos objetivos:* **Pesquisa Exploratória e Descritiva**<sup>1</sup>. As pesquisas exploratórias buscam uma abordagem do fenômeno pelo levantamento de informações que poderão levar o pesquisador a conhecer mais a seu respeito (GERHARDT; SILVEIRA, 2009). As pesquisas descritivas têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis (GIL, 1999);
- *Quanto aos procedimentos técnicos:* **Survey e Estudo de Caso**. De acordo com Gil (1999), as pesquisas deste tipo se caracterizam pela interrogação direta das pessoas cujo comportamento se deseja conhecer. Basicamente, procede-se à solicitação de informações a um grupo significativo de pessoas acerca do problema estudado para em seguida, mediante análise quantitativa, obter as conclusões correspondentes dos dados coletados. Ainda segundo Gil (1999), o estudo de caso é caracterizado pelo estudo exaustivo e em profundidade de poucos objetos, de forma a permitir conhecimento amplo e específico do mesmo; tarefa praticamente impossível mediante os outros delineamentos considerados.

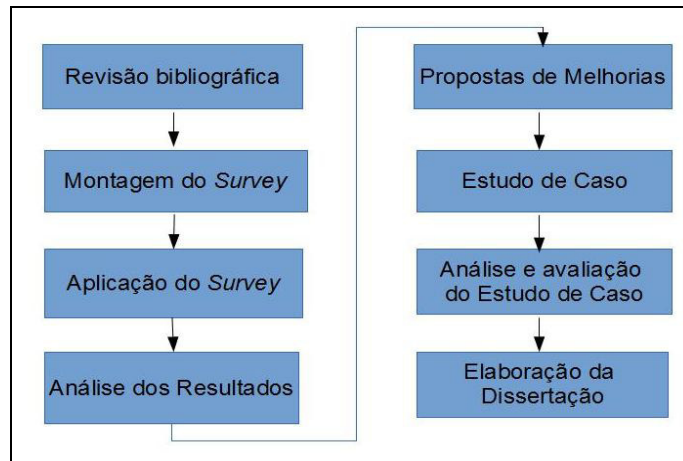
As etapas para execução da pesquisa, como observado na Figura 1, foram divididas em: revisão bibliográfica, montagem do *survey*, aplicação do *survey*, análise dos resultados, propostas de melhorias, estudo de caso, análise e avaliação do estudo de caso e elaboração da dissertação.

---

<sup>1</sup> Algumas pesquisas descritivas vão além da simples identificação da existência de relações entre variáveis, pretendendo determinar a natureza dessa relação. Neste caso tem-se uma pesquisa descritiva que se aproxima da explicativa. Por outro lado, há pesquisas que, embora definidas como descritivas a partir de seus objetivos, acabam servindo mais para proporcionar uma nova visão do problema, o que as aproxima das pesquisas exploratórias (GIL, 1999).



Figura 1- Etapas para elaboração da pesquisa



Fonte: O Autor

A primeira etapa consistiu na revisão bibliográfica e ocorreu durante todo o processo de elaboração da dissertação, pois novas publicações podem surgir e colaborar com o conteúdo da fundamentação teórica. É resultado de pesquisas bibliográficas em livros e artigos científicos relacionados ao assunto, por meio de consultas nas bases de dados *IEEE Xplore*, *ACM Digital Library* e periódicos avaliados pela CAPES. Serão considerados trabalhos que contenham informações acerca do alinhamento estratégico de TIC com a área de negócios e práticas de governança de TIC utilizadas pelas empresas.

A segunda etapa consistiu na montagem do *survey*, o qual teve como base o Questionário de Governança de TI 2014 aplicado pelo Tribunal de Contas da União (TCU) com vistas a obter o perfil de governança pública e de governança e gestão das aplicações, em órgãos e entidades federais, estaduais e municipais (TCU, 2015). Na aplicação do *survey*, terceira etapa, foi enviado (via *internet*) um questionário para os CIOs das empresas do estado de Sergipe durante os meses de outubro e novembro de 2015. A partir da aplicação do questionário permitiu-se analisar os resultados, quarta etapa, e montar um panorama preliminar das práticas de governança de TIC adotadas pelas empresas sergipanas.

Na quinta etapa foram realizadas pesquisas no âmbito das práticas de governança de TIC (ITIL, COBIT, PMBOK, BSC, CMMI entre outras) para a montagem das propostas de melhorias na Metodologia PETIC em relação à gestão de riscos e gestão da comunicação e transparência de TIC.

A sexta consistiu na realização do estudo de caso para avaliar a aplicabilidade e eficiência das melhorias propostas na Metodologia PETIC.

A sétima etapa consistiu na análise e avaliação dos resultados da realização do estudo de caso, registrando-se os pontos positivos e negativos das melhorias sugeridas. A viabilidade, aplicabilidade, aceitabilidade, aderência das melhorias propostas serão analisadas de acordo com o impacto e resultados obtidos. Ou seja, pretendeu-se verificar se as melhorias propostas podem ser aplicadas em uma organização e se os resultados obtidos são satisfatórios e permitem resolver os problemas de gestão de riscos e gestão da comunicação e transparência de TIC.

Por fim, a oitava e última etapa, a elaboração da dissertação, que evidenciou os resultados da pesquisa permitindo sua publicação e gerando oportunidades de outros estudos.

### **1.5.1.SURVEY**

Por se tratar de um trabalho em que o objetivo é proporcionar maior familiaridade com um problema ou situação, com vistas a torná-lo mais explícito ou aprimorar as ideias, o método de pesquisa utilizado neste estudo é o *survey*. A natureza quantitativa da pesquisa e o propósito exploratório descritivo no determinado período de tempo justificam esta opção.

Segundo Gerhardt e Silveira (2009) *apud* Fonseca (2002), a pesquisa com *survey* pode ser referida como sendo a obtenção de dados ou informações sobre as características ou as opiniões de determinado grupo de pessoas, indicado como representante de uma população-alvo, utilizando um questionário como instrumento de pesquisa.

Uma pesquisa tipo *survey* pode ter uma das três finalidades (MAY, 2014):

- Exploração - Têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou o aprimoramento de ideias;
- Explicação - Têm como preocupação central identificar os fatores que determinam ou contribuem para a ocorrência de determinados fenômenos;
- Descrição - Têm como objetivo primordial a descrição das características de determinado fenômeno, ou o estabelecimento de relações de variáveis.

### **1.5.2.ESTUDO DE CASO**

O estudo de caso enquadra-se como uma abordagem qualitativa e é frequentemente utilizado para coleta de dados na área de estudos organizacionais (LAKATOS; MARCONI, 2007).

Para Lakatos e Marconi (2007), o estudo de caso caracteriza-se por ser um tipo de pesquisa que apresenta como objeto uma unidade que se possa analisar de forma mais

aprofundada. Visa o exame detalhado de um ambiente, ou de um local, ou de uma situação qualquer, ou ainda de um determinado objeto, ou simplesmente de um sujeito ou de uma situação. Pode então ser conceituado como um modo de coletar informação específica e detalhada, frequentemente de natureza pessoal, envolvendo o pesquisador, sobre o comportamento de um indivíduo ou grupo de indivíduos em uma determinada situação e durante um período dado de tempo.

Frequentemente, o problema sob estudo preocupa-se mais em estabelecer as similaridades entre situações e, a partir daí, estabelecer uma base para generalização, o que muitas vezes justifica a generalização de um caso para outro, muito mais do que para uma população de casos (OLIVEIRA, 1997).

## 1.6 ORGANIZAÇÃO DA DISSERTAÇÃO

O texto dessa dissertação está organizado em seis capítulos. Os tópicos a seguir descrevem o conteúdo de cada um deles:

- Capítulo 1: Corresponde a esta introdução. Trata da contextualização, problemática e motivação, questões, objetivos, suposição, contribuições esperadas, metodologia de pesquisa e organização desta dissertação;
- Capítulo 2: Neste capítulo são discutidos os conceitos relacionados ao planejamento e ao alinhamento estratégico, práticas de governança de TIC, Metodologia PETIC, gestão de riscos e da comunicação e transparência de TIC;
- Capítulo 3: O capítulo descreve todos os passos executados para montagem, seleção dos participantes, execução do piloto, aplicação do *survey*, coleta, tabulação, análise dos dados e descrição das ameaças à validade da pesquisa;
- Capítulo 4: Apresenta a elaboração das propostas para incorporação da gestão de riscos e de comunicação e transparência de TIC e das alterações no *workflow* e componentes da Metodologia PETIC;
- Capítulo 5: Descreve e analisa a execução de um estudo de caso com o intuito de avaliar a utilização da Metodologia PETIC, com a inclusão da gestão de riscos e de comunicação e transparência de TIC, na elaboração do PE de TIC de uma empresa sergipana;
- Capítulo 6: Relata as considerações finais, principais contribuições, limitações do trabalho e trabalhos futuros.

## 2 REFERENCIAL TEÓRICO

---

Este capítulo aborda o referencial teórico, ou seja, a literatura sobre o planejamento estratégico, alinhamento estratégico, práticas de governança de TIC, Metodologia PETIC, gestão de riscos e da comunicação e transparência de TIC.

### 2.1 PLANEJAMENTO ESTRATÉGICO

Planejar origina-se na intenção de obter conhecimento utilizando métodos, análises e previsões para definir ações visando ao alcance de objetivos. Possibilita a mitigação dos riscos e ameaças ao crescimento fazendo uso de cenários, e assim, gera oportunidades de melhorias e manutenção no mercado (REZENDE, 2011).

De acordo com Drucker (1984, p.25):

[...] planejamento estratégico é um processo contínuo de, sistematicamente e com o maior conhecimento possível do futuro contido, tomar decisões atuais que envolvam riscos; organizar sistematicamente as atividades necessárias à execução destas decisões e, através de uma retroalimentação organizada e sistemática, medir o resultado dessas decisões em confronto com as expectativas alimentadas (DRUCKER, 1984. p25).

O conceito de estratégia refere-se aos planos da alta administração para alcançar resultados consistentes com a missão e os objetivos gerais da organização (WRIGHT *et al*, 2009).

O Planejamento Estratégico (PE) tem o objetivo de proporcionar bases necessárias para as manobras que permitem que as organizações naveguem e se perpetuem mesmo dentro de condições mutáveis cada vez mais adversas em seu contexto de negócios (CHIAVENATO; SAPIRO, 2004).

O PE está relacionado com os objetivos a médio e em longo prazo da organização, sendo revisado e ajustado conforme acordado com a alta direção. Trata-se de um contínuo processo de formulação de estratégias onde se objetiva a inserção da organização e de sua missão no ambiente onde está situada (LIMA, 2007).

O princípio fundamental do PE refere-se à alta direção analisar periodicamente se a organização deve oferecer os mesmos produtos e serviços, oferecer produtos e serviços novos e diferentes ou comercializar produtos e serviços de uma forma fundamentalmente diferente (JAANA *et al.*, 2012).

A partir do PE são determinados os objetivos e indicadores estratégicos considerando a análise econômica e estatística de períodos passados (avaliação do desempenho interno), bem

como a análise do ambiente externo relacionadas à visão e missão da empresa (KATAEV; BULYSHEVA, 2014).

Dentre os benefícios que o planejamento estratégico pode proporcionar, destaca-se (PALMEIRA, 2012 *apud* KOTLER, 1998):

- Pensamento sistemático no futuro e a melhoria das interações entre os gestores;
- Melhor definição dos objetivos e políticas organizacionais;
- Gerenciamento dos recursos necessários ao alcance dos objetivos;
- Padrões de desempenho mais fáceis de controlar;
- Previsão de ações corretivas, dentre outros.

## **2.2 PLANEJAMENTO ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**

O Planejamento Estratégico de Tecnologia da Informação e Comunicação (PE de TIC) pode ser definido como sendo o processo de identificação de infraestrutura (*hardware*, *software* básico e comunicação) e aplicações (banco de dados e automação de escritórios) para suportar o negócio das organizações, por meio do atendimento dos objetivos organizacionais (BRODBECK, 2001).

De acordo com Rezende (2011), a literatura apresenta vários termos para identificar o PE de TIC, tais como: Plano Diretor de Tecnologia da Informação (PDTI), Plano Diretor de Informática (PDI), Plano Estratégico de Tecnologia da Informação (PETI) ou Plano Estratégico de Sistemas de Informação (PESI).

Palmeira (2012) destaca as principais contribuições do PE de TIC, ressaltando que a sua efetividade depende do devido alinhamento às necessidades da organização:

- Melhoria do desempenho da área de TIC, seja pela alocação mais eficiente de recursos, como também pelo aumento de produtividade da equipe;
- Alinhamento das estratégias de TIC com as estratégias do negócio, possibilitando vantagens competitivas;
- Comprometimento da alta administração por intermédio da alocação dos recursos e resultados intermediários e incrementais;
- Antecipação de tendências futuras (inovação tecnológica contínua, evitando rupturas drásticas e altos investimentos);

- Aumento do nível de satisfação dos usuários, ofertando tecnologia compatível e com facilidade de manuseio.

A TIC promove mudanças estratégicas nas organizações a partir dos seguintes tipos de uso: redesenho do processo de negócio (realinhamento das atividades e relacionamentos em busca de maior desempenho), redesenho dos relacionamentos do negócio (agrega valor ao negócio em toda sua cadeia) e redefinição do escopo do negócio (VENKATRAMAN, 1997). Atualmente, a TIC tem sido reconhecida como uma ferramenta estratégica de competição, pois além de dar o suporte às operações de negócio, permite que se viabilizem novas estratégias (LAURINDO *et al.*, 2001).

Para BRODBECK (2001) alguns aspectos relacionados ao aumento das pressões dos negócios, dos riscos, das competências e da relação preço/performance, tem servido para mudar os papéis e funções de TIC, incluindo o seu uso para obtenção de vantagens competitivas e como transformadora dos processos, estrutura e relacionamento do negócio. Com isto, está se tornando difícil separar os aspectos de planejamento de TIC dos de negócio. É importante usar as ferramentas e técnicas de análise e planejamento estratégico de negócio para assegurar que o enfoque do planejamento estratégico de TIC esteja inter-relacionado com os padrões do gerenciamento estratégico do negócio.

Da mesma forma que as empresas devem ser flexíveis em relação aos seus processos organizacionais e a TIC ter a capacidade de se adequar às novas exigências do negócio, o PE de TIC deve ser flexível, dinâmico e adaptável. De acordo com Rezende (2011), o processo de elaboração do PE de TIC deve:

[...] permitir que todos os envolvidos da organização tenham condições de avaliar os produtos gerados nas subfases, registrando sua parcela de participação, para que o resultado do projeto seja de qualidade inquestionável e contribua com o alinhamento do planejamento dos sistemas de informação, dos sistemas de conhecimentos e da informática ao planejamento estratégico da organização. (REZENDE, 2011).

## **2.3 ALINHAMENTO ESTRATÉGICO ENTRE TIC E NEGÓCIO**

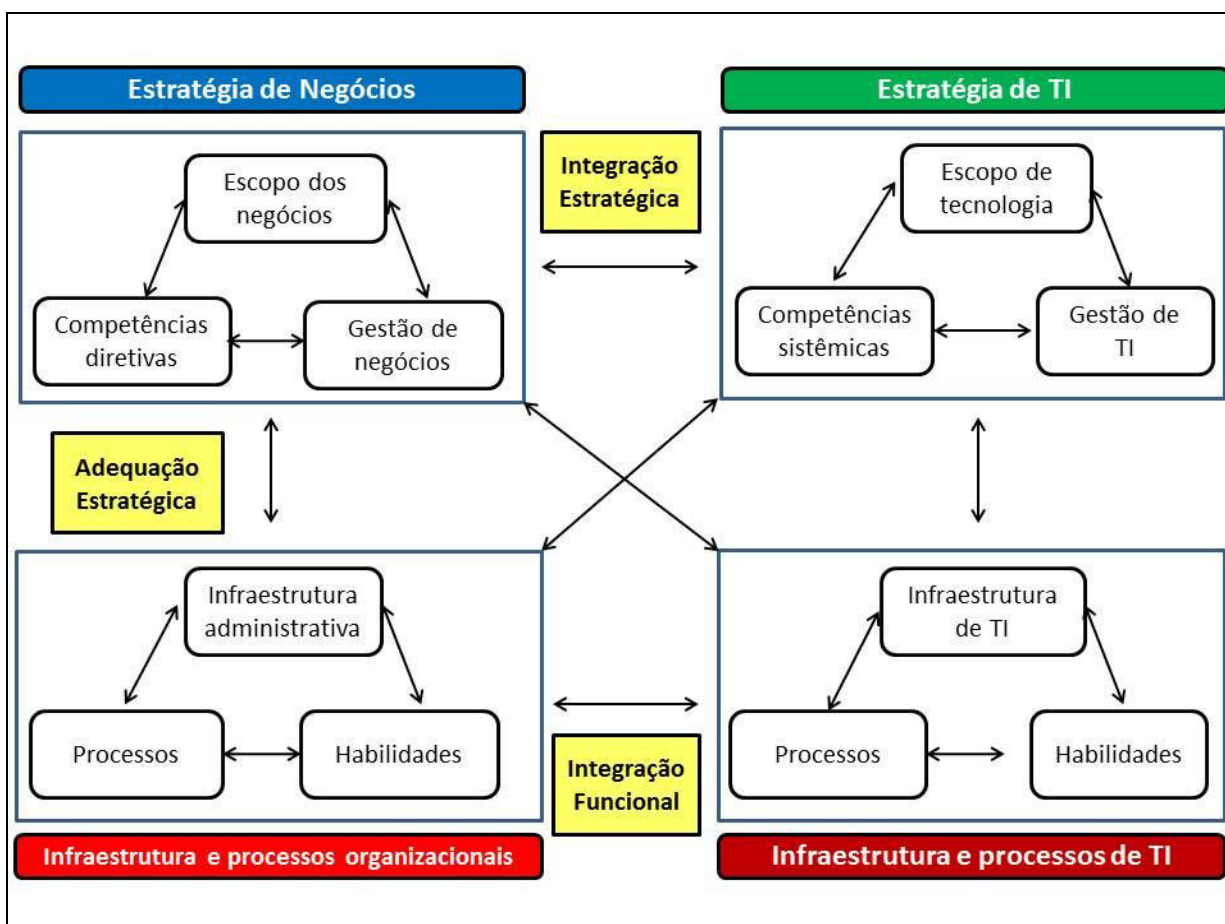
Segundo Rezende (2011), para implantação da estratégia de TIC se faz necessário o alinhamento estratégico entre o PE do negócio e o PE de TIC; a entrega de valor, que garante que a TIC entregue os prometidos benefícios previstos na estratégia da organização; a gestão de riscos, que busca assegurar que todas as ações e projetos estejam de acordo com o nível de risco esperado para o retorno que é proposto; gestão de recursos, a melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TIC (aplicativos,

informações, infraestrutura e pessoas); e, mensuração de desempenho, que monitora a implementação da estratégia, término do projeto, uso dos recursos, e entrega dos serviços.

O modelo do alinhamento estratégico entre os planos baseia-se em fatores internos e externos da organização, onde é feita análise do impacto de TIC nos negócios e também quais as disponibilidades de novas tecnologias que podem ser empregadas na organização (LAURINDO *et al.*, 2001).

Segundo Rezende (2011), o modelo de Henderson e Venkatraman (1993), ilustrado na Figura 2, é o modelo mais clássico, discutido e citado da literatura de alinhamento estratégico entre TIC e negócio. Ele é baseado em quatro domínios fundamentais: a) Estratégia de Negócio; b) Estratégia de TIC; c) Infraestrutura e Processos Organizacionais, e; d) Infraestrutura e Processos de TIC.

Figura 2- Modelo de Henderson e Venkatraman



Fonte: Rezende (2011).

Segundo Henderson e Venkatraman (1993), o alinhamento estratégico de TIC é baseado em duas condições:

1. Ajuste estratégico entre o posicionamento da organização e de TIC no mercado (ambiente externo) e a infraestrutura administrativa adequada para suportar tal posicionamento (ambiente interno);
2. Integração funcional entre os domínios de negócio e de TIC, tanto no nível estratégico quanto no nível de infraestrutura e processos.

Tendo por base o modelo de Henderson e Venkatraman (1993), Brodbeck e Hoppen (2003) propõem um novo modelo com promoção do alinhamento estratégico de TIC estendido à etapa de execução da estratégia. Ele contém um plano de frente, representando a promoção do alinhamento entre negócios e TIC durante a etapa de formulação do planejamento estratégico e vários planos de fundo, representando a promoção do alinhamento contínuo durante os diferentes estágios da execução da estratégia (implementação).

O modelo expressa duas formas de promoção do alinhamento contínuo. A primeira ocorre horizontalmente e de forma circular, entre os itens planejados de negócio e de TIC, indicando que o redirecionamento dos mesmos pode ser feito por ambos, a qualquer instante. A segunda ocorre linearmente, indicando o movimento dos itens planejados do estado presente para o futuro, implementando-se a visão básica de processo em movimento (BRODBECK; HOPPEN, 2003).

## 2.4 GOVERNANÇA DE TIC

A Governança de TIC cria e mantém processos e estruturas necessários para garantir a utilização eficaz e eficiente da TIC em uma organização visando atingir os objetivos de negócio (MAKHLOUF; ALLAL-CHERIF, 2015).

A literatura define Governança de TIC como a especificação das estruturas de tomada de decisão, processos e mecanismos relacionais para orientação e controle dos recursos de TIC. Identifica ainda como a habilidade organizacional, de grande importância para o alinhamento estratégico, agrega valor ao negócio por meio das TIC (BERMEJOA *et al.*, 2014).

A *Information System Audit and Control Association* (ISACA) define que a Governança de TIC consiste na estrutura de relações e de processos que apoiam o controle da empresa a fim de alcançar os objetivos corporativos por meio da mitigação de riscos e dos resultados obtidos com os recursos de TIC (ISACA, 2015). É o processo pelo qual a empresa alinha as ações de TIC com os seus objetivos de desempenho e presta contas destas ações e seus resultados (WEIL; ROSS, 2004). As práticas de Governança de TIC mais conhecidas e utilizadas no alinhamento estratégico de TIC e negócio são descritas no Quadro 1.



Quadro 1 - Práticas de governança de TIC

Prática	Descrição	Fonte
BSC	O <i>Balanced Scorecard</i> (BSC) é um modelo de gestão estratégica utilizado para medição e gestão de desempenho por meio de indicadores tendo como benefício o alinhamento destes aos objetivos da organização. Define quatro perspectivas: financeira, clientes, processos internos e aprendizado e crescimento.	(AZEVEDO, 2013); (MARCOS <i>et al.</i> , 2012)
CMMI	<i>Capability Maturity Model Integration</i> (CMMI) é um modelo baseado nas melhores práticas para o desenvolvimento e manutenção de produtos de <i>software</i> .	(CMMI, 2015); (PINHEIRO; MISAGHI, 2014);
COBIT	O <i>Control Objectives for Information and Related Technology</i> (COBIT) é definido como um conjunto de diretrizes baseadas em auditoria para processos, práticas e controles de TIC voltadas à redução de riscos, busca pela integridade, confiabilidade e segurança da informação. O COBIT ajuda a garantir o alinhamento entre TIC e objetivos de negócio da organização.	(ISACA, 2015); (ATESE; TANRIÖVER, 2014);(TEXTOR <i>et al.</i> , 2015); (PARVISI <i>et al.</i> , 2013); (KILIÇ; METIN, 2012)
ISO/IEC 27001-27002	As normas ISO/IEC 27001 ou 27002 são definidas para estabelecer, manter, operar, monitorar e melhorar um sistema de gestão de segurança da informação.	(AZEVEDO, 2013); (SHIVASHANKARA PPA <i>et al.</i> , 2012)
ITIL	<i>IT Infrastructure Library</i> (ITIL) é uma abordagem que fornece melhores práticas de controle sob a forma de processo. O ITIL é utilizado para a criação de uma estratégia de gerenciamento de serviços de TIC e orientação de profissionais na gestão eficaz dos recursos e serviços de qualidade de TIC.	(ITIL, 2015); (PARVISI <i>et al.</i> , 2013); (MAKHLOUF; ALLAL-CHERIF, 2015)
PE de TIC próprio ou customizado	PE de TIC próprio ou customizado é um mecanismo utilizado para planejar os processos e os recursos de TIC a fim de dar suporte aos processos de negócios e as estratégias da organização.	(BRODBECK, 2001)
PMBOK	<i>Project Management Body of Knowledge</i> (PMBOK) é um conjunto de melhores práticas que definem processos para o gerenciamento de projetos. Nele são encontradas orientações sobre as áreas que envolvem o projeto: escopo, tempo, custo, recursos humanos, comunicações, riscos, aquisições e qualidade.	(PMI, 2015); (MAKHLOUF; ALLAL-CHERIF, 2015)

Fonte: Autor (2017) baseado na revisão da literatura.

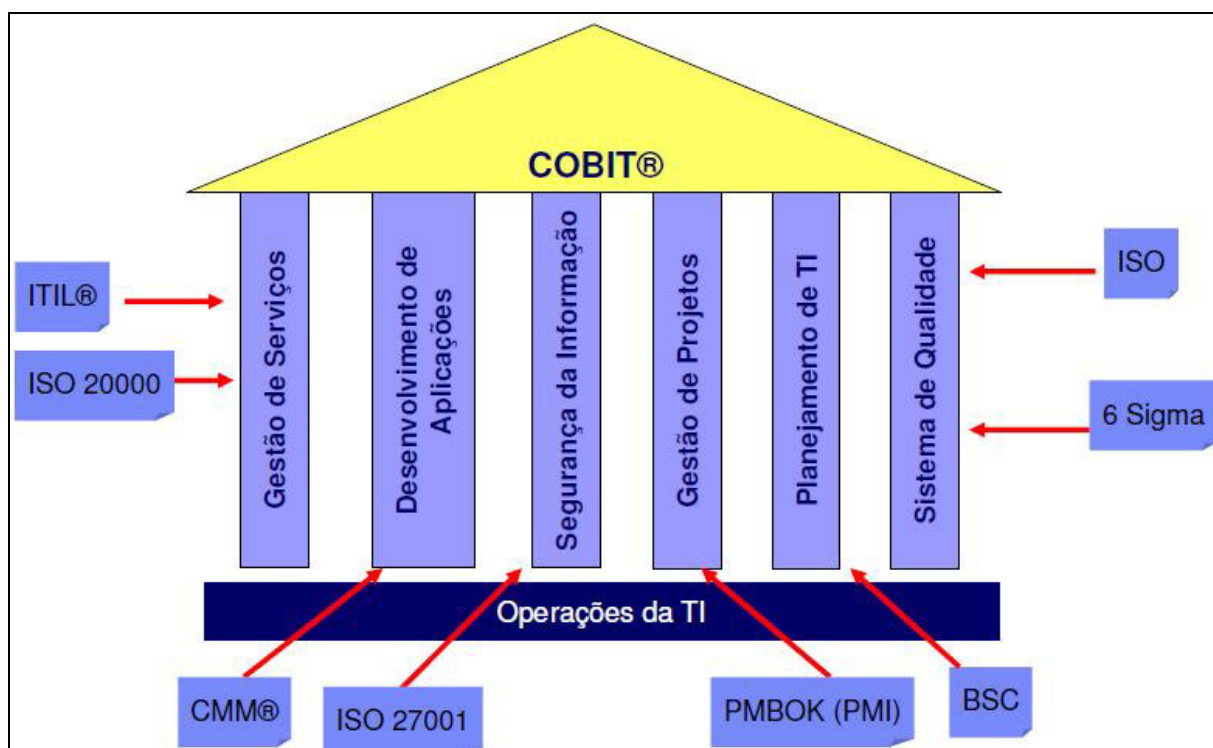
Os principais objetivos da Governança de TIC são alinhamento estratégico, agregação de valor, gerenciamento de recursos, gestão de riscos e gestão da mensuração de desempenho (PARVISI *et al.*, 2013).

Segundo Palmeira (2012), a Governança de TIC vem sendo adotada com a utilização de alguns *frameworks* e modelos. Dentre eles merecem destaque o COBIT, a ISO 38500 e o VAL IT. Para dar suporte ao uso de tais *frameworks* e a efetiva implantação de Governança de TIC, vários outros modelos são usados como mecanismos complementares. A Figura 3 ilustra os principais modelos e suas respectivas áreas focais. Essas práticas visam auxiliar o processo de

implantação da Governança de TIC e, conseqüentemente, dar suporte ao PE de TIC e ao alinhamento estratégico entre TIC e negócio. Como a escolha delas depende muito do tipo de negócio da organização, elas podem ser agrupadas conforme:

- Para gestão dos serviços: ITIL e ISO;
- Para melhoria do processo de *software*: CMMI;
- Para segurança da informação: ISO família 27000;
- Para gestão de projetos: PMBOK;
- Para o planejamento estratégico de TIC: BSC e PE de TIC próprio ou customizado;
- Para gestão dos processos, atividades de controle, otimização dos investimentos, entrega de produtos e serviços de TIC: COBIT.

Figura 3- Governança de TIC



Fonte: Palmeira (2012).

## 2.5 METODOLOGIA PETIC

A Metodologia PETIC foi concebida como uma alternativa adequada na implementação de um PE de TIC em organizações públicas ou privadas de qualquer porte (MARCHI, 2010; NASCIMENTO, 2011).

A PETIC representa um conjunto de normas e diretrizes para a concepção de um PE voltado para as TIC dentro das organizações e aborda as seis grandes áreas (ou os seis pilares) dos Sistemas de Informação, a saber: (i) Dados, (ii) *Software*, (iii) *Hardware*, (iv) Telecomunicações, (v) Pessoas, (vi) Governança de TIC (PALMEIRA, 2012).

A denominação PETIC surgiu a partir de um trabalho acadêmico realizado por um grupo de alunos numa disciplina optativa do DCOMP da UFS em meados de 2008. Naquele trabalho foi criado um PE para ser aplicado no estudo de caso escolhido: o Centro de Processamento de Dados (CPD) da UFS. Este trabalho teve como propósito auxiliar o CPD da UFS a atingir suas metas por meio do planejamento estruturado de suas TIC, produzindo mais, com menos esforço (MARCHI, 2010; NASCIMENTO, 2011).

### 2.5.1. OS COMPONENTES DA METODOLOGIA PETIC

Os componentes da Metodologia PETIC, ilustrados na Figura 4, são: (i) Catálogo de Processos de TIC, (ii) Repositório de Ações de TIC, (iii) Catálogo de Ferramentas e Técnicas, (iv) Artefato PETIC, (v) Gráficos de Custos versus Importância, (vi) Mapas de Gantt dos pilares de Sistemas de Informação (SI) e o (vii) *software* PETIC Wizard. (PALMEIRA, 2012).

Figura 4- Componentes da Metodologia PETIC



Fonte: Palmeira (2012).

### 2.5.2. CATÁLOGO DE PROCESSOS DE TIC

O Catálogo de Processos objetiva manter um repositório centralizado de processos de TIC. Ele é continuamente atualizado à medida que a metodologia é aplicada nas organizações.

Adicionalmente, utiliza como referência os processos do COBIT e de outros modelos e *frameworks* de Governança de TIC como ITIL, CMMI/MPS.BR e PMBOK (PALMEIRA, 2012).

### **2.5.3. REPOSITÓRIO DE AÇÕES**

O componente Repositório de Ações é usado como referência para o gestor na definição das ações de melhoria de processos durante a elaboração do artefato PETIC. Deverá contemplar todas as ações possíveis, referentes a cada processo de TIC. Incorpora soluções e recomendações de várias organizações e, além disso, também utiliza os modelos e *frameworks* de Governança de TIC (PALMEIRA, 2012).

### **2.5.4. CATÁLOGO DE FERRAMENTAS E TÉCNICAS**

Contém um conjunto de ferramentas e técnicas que visa auxiliar gestores e consultores durante a aplicação da metodologia. Objetiva fornecer instrumentos de apoio em cada passo da metodologia, incluindo atividades de elaboração, implementação e monitoramento e controle do planejamento (PALMEIRA, 2012).

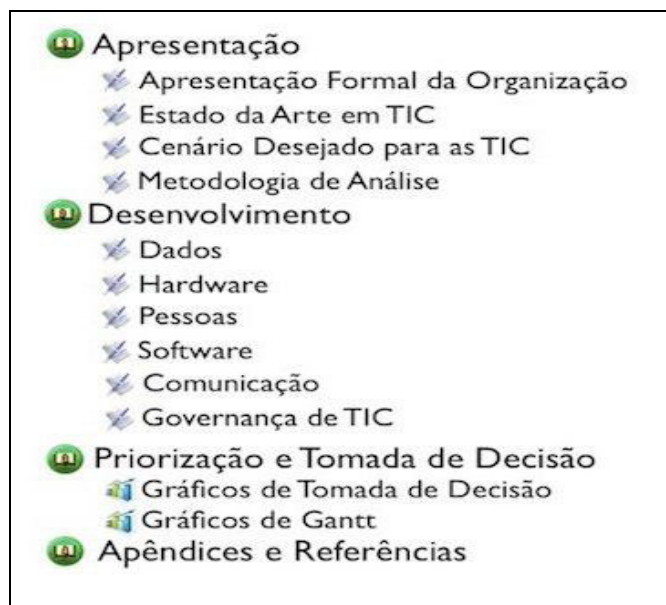
### **2.5.5. O ARTEFATO PETIC**

A produção artefato PETIC de uma organização requer a criação de um grupo de trabalho ou de equipes de trabalho que possam analisar os pilares da metodologia: (dados, pessoas, telecomunicações, *hardware*, *software* e Governança de TIC) (MARCHI, 2010; PALMEIRA, 2012).

Estes pilares são os responsáveis pela execução das atividades de entrada, processamento, saída, armazenamento e controle de dados e, em seguida, a consequente transformação desses dados em produtos de informação (MARCHI, 2010; PALMEIRA, 2012).

O primeiro passo importante na criação do artefato é descobrir a missão, a visão e os valores do setor/unidade de TIC da organização, assim como a análise do ambiente, a razão da sua existência, as atribuições de cada gerente, do diretor e até dos secretários (MARCHI, 2010; PALMEIRA, 2012).

Figura 5 - Artefato PETIC



Fonte: Palmeira (2012).

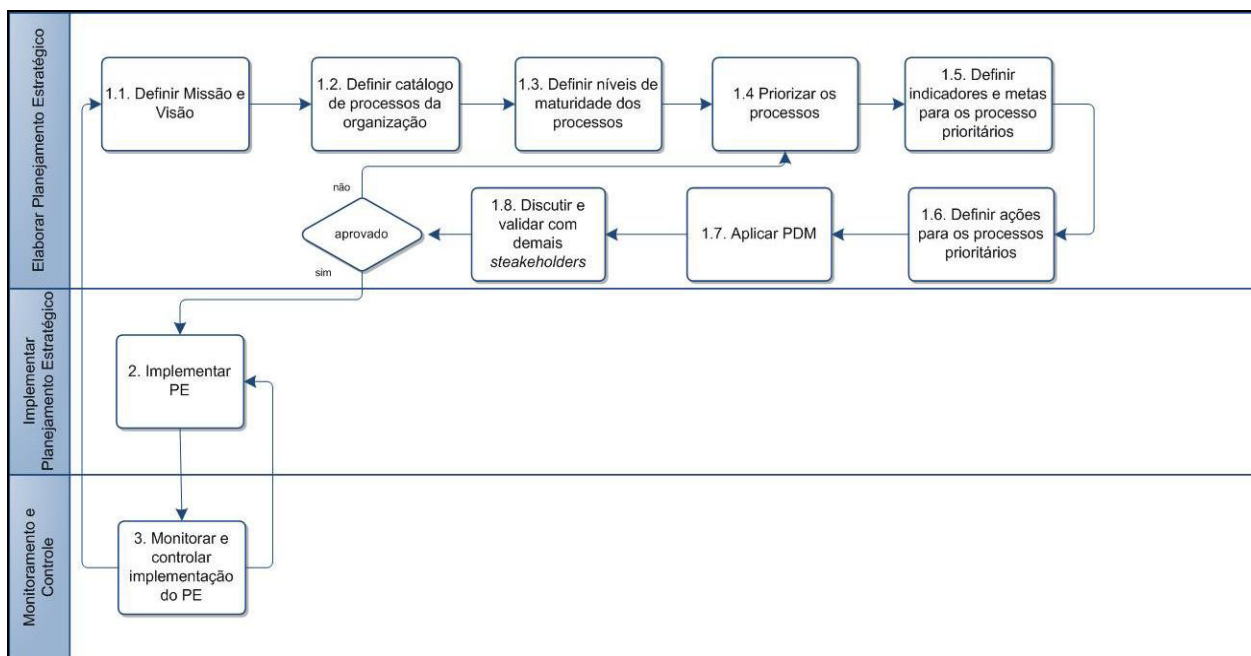
A Figura 5 mostra o Artefato PETIC dividido em duas partes, sendo a primeira a “Apresentação da Organização” onde são mostradas: (i) a parte formal da organização (ramo, atividades, estrutura organizacional, missão e visão); (ii) o estado da arte em TIC (descrição das novas tecnologias que serão aplicadas no cenário desejado das seis grandes áreas); (iii) cenário desejado para os processos de TIC na Organização (resumo do alinhamento do estado da arte em TIC com os pilares de SI da organização); e (iv) a metodologia de análise do PETIC (nomes e cargos das pessoas envolvidas e a metodologia de análise das informações que foram aplicadas) (MARCHI, 2010; PALMEIRA, 2012).

A segunda parte é o Desenvolvimento, onde são descritos o cenário atual, a descrição do cenário desejado e as prioridades, custos e execução de cada atividade planejada. As informações levantadas referem-se aos pilares: (i) dados (banco de dados, *backup*, redundância, *data warehouse* e segurança; (ii) *hardware* (*desktops*, *notebooks*, *nobreaks*, *datashows*, *benchmark*, proteção contra sinistros, aquisição e suporte); (iii) gestão de pessoas (contratação, treinamentos, salários, ergonomia, cargos, avaliação de desempenho e segurança no local de trabalho); (iv) *software* (sistemas operacionais, desenvolvimento, aquisição e *frameworks* e métodos de acesso), (v) telecomunicações (VoIP, *backbones*, pontos de acesso, arquitetura e segurança da rede, rádio, tv e blogs) e governança de TIC (MARCHI, 2010; PALMEIRA, 2012).

## 2.5.6. O WORKFLOW DA METODOLOGIA PETIC

Segundo a metodologia, o PE de TIC é consolidado em um documento chamado Artefato PETIC. O fluxo de trabalho detalhado, contendo as suas tarefas, é mostrado na Figura 6.

Figura 6 - Etapas detalhadas do PE



Fonte: Rocha (2017).

Seguindo corretamente o *workflow*, o fluxo de trabalho proposto pela Metodologia PETIC passa a ser interativo e engloba o que ocorre na prática durante a execução das atividades (PALMEIRA, 2012).

## 2.6 GESTÃO DE RISCOS DE TIC

A gestão de riscos de TIC existe para prever, lidar e amenizar os riscos relacionados com a área de TIC e suas diversas aplicações. É composta de ações formalizadas e coordenadas para controlar um conjunto de ativos, instalações, processos e pessoas com relações e responsabilidades definidas (PMI, 2015).

Segundo Carissimi (2017), a gestão de riscos é um modelo que busca lidar com uma realidade complexa, um alvo móvel em constante transformação. Pode induzir ao erro, quando resulta em uma falsa sensação de conforto e de segurança. Os inúmeros ataques cibernéticos bem-sucedidos noticiados frequentemente são uma prova de que algo não está funcionando, apesar de contínuos esforços em gestão de riscos e implementação de controles.

A seguir serão apresentadas como as práticas de governança de TIC identificadas no *Survey* abordam a gestão de riscos em suas metodologias.

### 2.6.1. ABORDAGEM PMBOK

Para o PMBOK, risco é um evento ou uma condição incerta que, se ocorrer, tem um efeito em pelo menos um objetivo do projeto. Podem incluir escopo, cronograma, custo e qualidade. Esta é uma área essencial para aumentar as taxas de sucesso dos projetos, pois todos eles possuem riscos e precisam ser gerenciados, ou seja, saber o que pode causar impacto e saber o que fazer com cada um deles. A gestão de riscos inclui os seguintes processos: a) planejar o gerenciamento de riscos; b) identificar os riscos; c) realizar a análise qualitativa dos riscos; d) realizar a análise quantitativa dos riscos; e) planejar as respostas aos riscos; f) controlar os riscos (PMI, 2015).

O planejamento do gerenciamento de riscos é o processo de definição de como conduzir as atividades de gerenciamento de riscos de um projeto. O processo de identificação dos riscos determina os que podem afetar o projeto e a documentação das suas características (PMI, 2015).

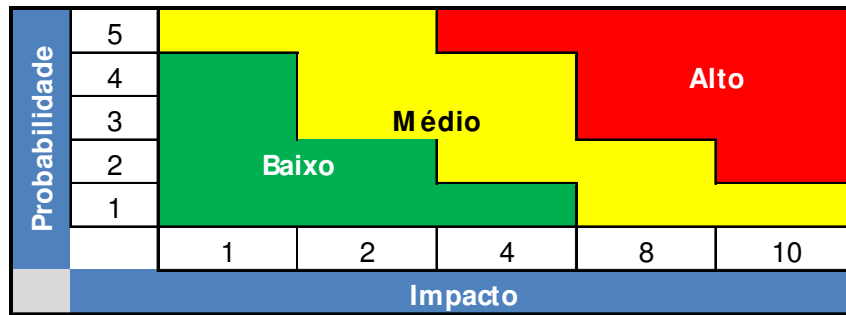
A realização da análise qualitativa dos riscos representa a avaliação da severidade do risco, ou seja, a combinação de sua probabilidade de ocorrência com o impacto causado.

De acordo com o PMI (2015), a probabilidade de ocorrência de um risco pode ser: *muito baixa* (probabilidade mínima de ocorrência do risco); *baixa* (pode haver ocorrência do risco, mas é improvável); *média* (provavelmente o risco irá ocorrer); *alta* (muito provável que o risco ocorra); *muito alta* (espera-se a ocorrência do risco).

De modo análogo, o impacto causado pela ocorrência do risco é classificado como: *muito baixo* (impacto limitado, sem grandes consequências); *baixo* (baixo impacto, mas com alguma interferência no processo); *médio* (impacto moderado que requer intervenções); *alto* (alto impacto nas operações, representando ameaças); *muito alto* (impacto significativo, representando interrupções do processo) (PMI, 2015).

A matriz de prioridade, ilustrada na Figura 7, é obtida pelo produto da probabilidade com o impacto de ocorrência do risco, resultando no grau de prioridade: *baixo*, *médio* ou *alto*. Para tanto, é atribuído um peso de 1 a 5 para cada alternativa da probabilidade. No caso do impacto, os pesos são respectivamente 1, 2, 4, 8 e 10.

Figura 7 - Matriz de prioridade (probabilidade x impacto)



Fonte: PMI (2015)

No que se refere ao processo de análise qualitativa dos riscos, o PMBOK sugere realizar as seguintes análises (PMI, 2015):

- Impacto Financeiro – representa o montante financeiro necessário para contingenciamento do risco diante de sua ocorrência;
- Valor Monetário Esperado (VME)<sup>2</sup> - conceito estatístico que identifica e calcula o resultado médio quando o futuro inclui cenários que podem ocorrer ou não;
- Reserva de Contingência (RC) – representa o somatório dos VMEs de todos os riscos analisados que constará no orçamento anual diante da impossibilidade de reservar o total do impacto financeiro de todos os riscos avaliados.

O planejamento das respostas aos riscos desenvolve as opções e ações para aumentar as oportunidades e reduzir as ameaças aos objetivos do projeto. Em relação ao planejamento das respostas, o PMI (2015) indica que:

- Assumir o risco - significa que não será criado nenhum plano ou ação para tentar evitar ou mitigar o risco, preferindo aceitar as suas consequências, seja porque não é possível elaborar estratégia adequada de resposta ou porque os custos da ação de prevenção são maiores que o dano causado pelo evento de risco ou pelo fato da probabilidade e o impacto serem muito baixos;
- Mitigar o risco – busca reduzir a probabilidade de ocorrência e o impacto de um evento de riscos para níveis aceitáveis. Permite reduzir a ameaça por meio do planejamento de alternativas de modo a evitá-lo ou reduzir seu impacto caso ele se concretize. A finalidade da mitigação é diminuir a probabilidade de ocorrência e o impacto do risco até um nível que lhe permita absorver suas consequências;
- Evitar o risco – implica em procurar evitar o risco por completo, eliminando a causa dos eventos de risco;

<sup>2</sup>VME = Probabilidade de Ocorrência do Risco x Impacto Financeiro do Risco



- Transferir o risco – representa transferir os riscos e suas consequências para terceiros. Não se elimina o risco, mas transfere-se a responsabilidade por seu gerenciamento.

No caso de um risco possuir um grau de severidade baixo, orienta-se assumir o risco. Sendo grau médio, pode-se assumi-lo ou mitigá-lo. E, sendo grau alto, pode-se evitá-lo, mitigá-lo ou transferi-lo (PMI, 2015):

Por fim, controlar o risco é o processo de implementação de planos de respostas aos riscos, acompanhando os riscos identificados, monitorando riscos residuais, identificando riscos secundários e avaliando a eficácia do processo de gerenciamento de riscos durante todo o projeto (PMI, 2015).

O PMI (2015) diferencia risco residual de risco secundário. O risco residual é um risco remanescente, aquele risco mínimo que ainda permanece após a implementação de uma resposta a um risco. Já o risco secundário surge em decorrência da efetivação de uma resposta ao risco.

## **2.6.2. ABORDAGEM ITIL**

A ITIL não trata o risco diretamente, mas no que chama de Gerenciamento da Continuidade dos Serviços de TI (GCSTI) faz referência a desastres ou riscos de eventos que podem causar desastres. O objetivo do GCSTI é dar suporte ao Gerenciamento da Continuidade de Negócio (GCN) assegurando que os requisitos técnicos da TIC e facilidades de determinados serviços possam ser recuperados dentro de prazos requeridos e acordados (ITIL, 2015).

Enquanto o GCN gerencia os riscos assegurando a continuidade da organização com um nível mínimo estabelecido em casos de desastres, o GCSI atua para que o mínimo de serviços de TIC possam ser disponibilizados. O processo de GCSI é composto por quatro estágios (ITIL, 2015):

1. Iniciação;
2. Requisitos e estratégia;
3. Implementação;
4. Gerenciamento operacional.

Segundo o ITIL (2015), a Iniciação contempla a organização como um todo. As políticas ao redor do GCN e do GCSI são identificadas, o escopo do processo e os termos de referências são determinados, recursos alocados e um plano de projeto estabelecido. A etapa Requisitos e estratégia se divide em:

- Análise de impacto do negócio – investiga-se o impacto do desastre no negócio;
- Avaliação do risco – analisa a probabilidade de um desastre ou outra interrupção ocorrer. Avalia-se o nível de perigo e extensão da insegurança da organização. Analisa as vulnerabilidades e as ameaças para todos os ativos críticos. No gerenciamento de risco, que se preocupa em identificar os contra recursos para manter os riscos sob controle e, sendo o caso, pode representar ações para redução do impacto ou probabilidade do risco, desenvolvendo planos de recuperação, os quais detalham como agir quando os riscos ocorrerem.
- Estratégia e continuidade dos negócios – representa a estratégia apropriada para redução dos riscos e opções de recuperação. No caso de um plano de recuperação, as decisões devem ser feitas acerca da recuperação: i) nenhuma contingência; ii) procedimentos administrativos; iii) estratégia de fortificação; iv) arranjos recíprocos; v) recuperação gradual (*cold stand-by*); vi) recuperação intermediária (*warm stand-by*); recuperação imediata (*hot stand-by*).
- Implementação - consiste em: i) organização e plano de implementação, que necessitam ser criados para implantação dos processos; ii) implantar arranjos *stand-by* e medidas de redução de riscos; iii) desenvolver planos e procedimentos de GCSTI, definindo-se o plano de recuperação (quando será atualizado, lista de responsáveis por definir qual ação deve ir para determinado grupo); iv) iniciação da recuperação; v) grupo de especialistas (administração, pessoal de infraestrutura de TIC, segurança, sites de recuperação e restauração); vi) execução dos testes iniciais para verificar se a estratégia escolhida funciona;
- Gerenciamento operacional – consiste em: i) educação, treinamento e conscientização; ii) revisão e auditoria; iii) testes; iv) gerenciamento de mudanças; v) garantia, ou seja, verificação da qualidade do processo para assegurar que os requisitos do negócio sejam alcançados.

### 2.6.3. ABORDAGEM COBIT

Para o COBIT, segundo ISACA (2015), qualquer impacto em potencial nos objetivos da empresa causado por um evento não planejado deve ser identificado, analisado e avaliado. Estratégias de mitigação de risco devem ser adotadas para minimizar o risco residual a níveis aceitáveis. O resultado da avaliação deve ser entendido pelas partes interessadas e expresso em

termos financeiros para permitir que as partes interessadas alinhem o risco a níveis de tolerância aceitáveis. Os objetivos desse processo são:

- Alinhamento da gestão de riscos de TIC e de negócios - estabelecer uma estrutura de gestão de riscos de TIC alinhada com a estrutura de gestão de riscos da organização;
- Estabelecimento do contexto de risco - estabelecer o contexto ao qual a estrutura de avaliação de risco é aplicada para assegurar resultados esperados. Isso inclui a definição dos contextos interno e externo de cada avaliação de risco, o objetivo da avaliação e os critérios pelos quais os riscos são avaliados;
- Identificação de eventos - identificar eventos com potencial impacto negativo nos objetivos ou nas operações da organização, incluindo aspectos de negócios, regulamentação, aspectos jurídicos, tecnologia, parcerias de negócio, recursos humanos e operacionais. Determinar a natureza do impacto e manter esta informação. Registrar e manter um histórico dos riscos relevantes;
- Avaliação de risco - avaliar regularmente a probabilidade e o impacto de todos os riscos identificados, utilizando métodos qualitativos e quantitativos. A probabilidade e o impacto associado ao risco inerente e residual devem ser determinados individualmente, por categoria e com base no portfólio da organização;
- Resposta ao risco - desenvolver e manter um processo de respostas a riscos para assegurar que controles com uma adequada relação custo-benefício mitiguem a exposição aos riscos de forma contínua. O processo de resposta ao risco deve identificar estratégias de risco, tais como evitar, reduzir, compartilhar ou aceitar o risco, determinar responsabilidades, e considerar os níveis de tolerância definidos;
- Manutenção e monitoramento do plano de ação de risco - priorizar e planejar as atividades de controle em todos os níveis da organização para implementar as respostas aos riscos identificadas como necessárias, incluindo os custos, benefícios e responsabilidade pela execução. Obter aprovações para ações recomendadas e aceitação de quaisquer riscos residuais, e assegurar que as ações aprovadas sejam assumidas pelos donos dos processos afetados. Monitorar a execução dos planos e reportar qualquer desvio para a alta direção.

#### **2.6.4. ABORDAGEM CMMI**

O gerenciamento de riscos é efetivamente tratado por meio da área de processo *Risk Management* (gerência de riscos). Esta área de processo atua de uma forma proativa no sentido de minimizar os impactos dos riscos nos objetivos do projeto (CMMI, 2015):

- Preparar-se para a gerência de riscos –tem a função de estabelecer uma estratégia para identificar, analisar e mitigar riscos, que deverão ficar documentadas num plano de gerenciamento de riscos;
- Identificar e analisar riscos - tem a função de identificar os riscos e categorizá-los, além de fazer a sua análise para obter o nível de probabilidade e impacto, com o objetivo de priorizá-los quanto ao seu grau de criticidade;
- Mitigar riscos - tem a função de atuar nos riscos no sentido de minimizar a sua probabilidade de ocorrência e o seu impacto aos objetivos do projeto.

#### **2.6.5. ABORDAGEM ISO 27005**

A ISO 27005 fornece as diretrizes para o gerenciamento de riscos de segurança da informação (SI) e dá sustentação aos conceitos especificados na ISO 27001:2005, a norma de requisitos de sistemas de gestão da SI, além de auxiliar sobremaneira na implementação e certificação de tais sistemas de gestão.

Segundo a ISO 27005 o processo de gestão de riscos de segurança da informação tem por base as seguintes etapas:

- Definição do contexto–responsável pela definição do ambiente e todas as informações relevantes, escopo, ou seja, o conjunto de ativos, ameaças e vulnerabilidades que serão gerenciadas e os critérios de avaliação;
- Análise e avaliação de riscos – identificação dos riscos e a determinação das ações necessárias para tornar os riscos aceitáveis. Os riscos são identificados, estimados e avaliados;
- Tratamento do risco – dependerá da avaliação do risco e definirá a ação a ser tomada: a) reduzir o risco; b) reter o risco; c) evitar o risco; d) transferir o risco;
- Aceitação do risco – assegura os riscos aceitos pela organização, ou seja, os riscos que por algum motivo não serão tratados ou serão tratados parcialmente. São classificados como riscos residuais;

- Comunicação do risco – os riscos são comunicados para todas as áreas funcionais e seus gestores e como serão tratados;
- Monitoramento e análise crítica - são realizadas atividades de acompanhamento dos resultados, implementação dos controles e análise crítica do processo de melhoria contínua dos processos de gestão de riscos.

#### 2.6.6. COMPARATIVO DAS ABORDAGENS

O Quadro 2 abaixo apresenta o resumo do comparativo da gestão de riscos diante das diversas abordagens das práticas de Governança de TIC.

Quadro 2- Comparativo das abordagens da gestão de riscos

ITIL	PMBOK	COBIT	ISO 27005	CMMI
Análise de impacto no negócio	Planejamento da gerência de riscos	Alinhamento da gestão de riscos de TIC e de negócio Estabelecimento do contexto de riscos	Definição do contexto	Determinar fontes e categorias de riscos Definir parâmetros de risco Estabelecer estratégia para gerência de risco
Avaliação de risco	Identificação dos riscos	Identificação de eventos	Análise e avaliação de riscos	Identificar e analisar risco
	Análise qualitativa dos riscos	Avaliação de risco	Aceitação do risco	
	Análise quantitativa dos riscos			
Estratégia de contingência dos serviços	Planejamento das respostas aos riscos	Resposta ao risco	Definição do plano de tratamento do risco	Desenvolver planos de mitigação de riscos
Implementação	Monitoramento e Controle dos Riscos	Manutenção e monitoramento do plano de ação de risco	Implementar plano de tratamento do risco	Implementar os planos de mitigação de riscos
Gerenciamento operacional	Monitoramento e controle dos riscos	Manutenção e monitoramento do plano de ação de risco	Monitoramento contínuo e análise crítica dos riscos	
			Manter e melhorar o processo de gestão de riscos de segurança da informação	

Fonte: Autor (2017).

## 2.7 GESTÃO DA COMUNICAÇÃO E TRANSPARÊNCIA DE TIC

Cada comunicação deve ter seu conteúdo definido, avaliado e classificado. Isso porque a informação pode não ser destinada a todos. O conteúdo da comunicação ou mensagem pode ser um fato, ideias, emoções, dados, notícias, documentos, imagens, sons, arquivos ou qualquer outro conteúdo que se deseja comunicar (ISACA, 2015; PMI, 2015; WEIL; ROSS, 2005).

A gestão da comunicação e transparência de TIC tem como objetivo difundir por toda a organização as decisões e processos de governança de TIC e os respectivos comportamentos desejáveis. Entre as principais abordagens de comunicação estão (WEIL; ROSS, 2005):

- Comunicação da alta gerência - comunicados que esclarecem prioridades e demonstram comprometimento. A responsabilidade e a clareza quanto ao que será ou não será feito ajuda todos a concentrar sua atenção nos objetivos estratégicos;
- Comitês formais - além da participação nas decisões no nível executivo, os comitês também tomam decisões de governança de níveis inferiores e incumbem-se de decisões de alto nível;
- Escritório da Governança de TIC - fornece um responsável à Governança de TIC, assegurando que os mecanismos individuais se reforcem uns aos outros, ao invés de se contradizerem, e comunica os processos e propósitos da governança;
- Portais baseados na *web* - proveem um canal central de comunicação para as empresas. Os portais aumentam a transparência da governança ao disponibilizar as políticas, os padrões, o desempenho e algumas vezes os debates da empresa.

A seguir serão apresentadas como as práticas de governança de TIC identificadas no Survey abordam a comunicação e transparência em suas metodologias.

### 2.7.1. ABORDAGEM PMBOK

Segundo o PMBOK, a área de conhecimento Gerenciamento das Comunicações inclui os processos necessários para assegurar que as informações do projeto sejam planejadas, coletadas, criadas, distribuídas, armazenadas, recuperadas, gerenciadas, controladas, monitoradas e finalmente dispostas de maneira oportuna e apropriada (PMI, 2015). Esta área possui três processos:

- Planejar o gerenciamento das comunicações — o processo de desenvolver uma abordagem apropriada e um plano de comunicações do projeto com base nas

necessidades de informação e requisitos das partes interessadas, e nos ativos organizacionais disponíveis;

- Gerenciar as comunicações — o processo de criar, coletar, distribuir, armazenar, recuperar e de disposição final das informações do projeto de acordo com o plano de gerenciamento das comunicações;
- Controlar as comunicações — o processo de monitorar e controlar as comunicações no decorrer de todo o ciclo de vida do projeto para assegurar que as necessidades de informação das partes interessadas do projeto sejam atendidas.

Segundo o PMI (2015), a comunicação é classificada como:

- Confidencial – mais alto nível de confidencialidade e disponível para um grupo limitado de pessoas dentro da organização;
- Restrita – possui um nível médio de confidencialidade, restrita a um grupo um pouco mais amplo de pessoas;
- Uso interno – é o nível mais baixo de confidencialidade e determina que a informação circule no âmbito interno seja do setor, departamento ou organização;
- Pública – neste caso, a informação pode ser disponibilizada para todos.

O canal de comunicação é o meio pelo qual a mensagem é enviada do emissor para o receptor. Sua utilização dependerá da disponibilidade e recursos da organização e do conteúdo que se deseja comunicar (PMI, 2015). Alguns meios de comunicação citados são: documentos eletrônicos; sistemas de informação / base de dados; relatórios; documentos em papel; mídias de armazenamento (discos, cartões de memórias, fitas, etc.); Informação transmitida verbalmente; portais de Comunicação / *Sites (intranet e internet)*; sistema de bate-papo ou comunicadores instantâneos; mensagens eletrônicas; *e-mails*; vídeo ou teleconferências; painéis eletrônicos; murais ou quadros.

É necessário se contemplar a periodicidade em que a comunicação da informação deve ser enviada, mantendo-a atualizada constantemente (PMI, 2015). A periodicidade pode ser permanente ou contínua; sempre que necessária; periodicamente (segundos, minutos, horas, dias, meses, anos, *etc.*).

### **2.7.2. ABORDAGEM ITIL**

Para ITIL (2015), a comunicação deve ser ampla o suficiente para que seja atingindo o seu público alvo, já que o processo de comunicação só é estabelecido quando o receptor capta o

que o emissor deseja transmitir. Deve ter um objetivo definido e servirá como um meio de prevenção e diminuição de qualquer tipo de problema operacional e ocorrer de modo formal.

A efetividade do processo de comunicação só ocorrerá a partir da definição dos meios de comunicação apropriados para a organização, como por exemplo, *e-mail*, *folders*, mensagens, *intranet* e com definição de um fluxo de atividade, com o responsável pela redação, envio, aprovação e revisão da mensagem. Além disso, deve obrigatoriamente considerar os requisitos de segurança.

Ainda segundo ITIL (2015), o treinamento e formas de conscientização compreendem o processo de comunicação e devem ser utilizados em novos processos organizacionais, ferramentas, normas, procedimentos e todo objetivo estratégico.

### **2.7.3. ABORDAGEM COBIT**

O COBIT possui o processo “PO6 Comunicar Metas e Diretrizes Gerenciais”. A Direção deve desenvolver uma estrutura de controle de TIC corporativa e definir e comunicar políticas. Um programa de comunicação contínuo aprovado e apoiado pela alta direção deve ser implementado para articular missão, metas, políticas, procedimentos, etc. A comunicação apoia o alcance dos objetivos de TIC e assegura a consciência e o entendimento dos negócios, dos riscos de TIC, dos objetivos e das diretrizes. O processo deve assegurar conformidade com leis e regulamentos relevantes (ISACA, 2015).

O processo de Comunicação deve satisfazer os requisitos do negócio para TIC, mantendo as informações precisas e atualizadas nos serviços de TIC atuais e futuros. Dentre os objetivos e controles detalhados desse processo de Comunicação, destacam-se (ISACA, 2015):

- PO6.3 - Gerenciamento de políticas de TIC - desenvolver e manter um conjunto de políticas para apoiar a estratégia de TIC. Essas políticas devem incluir os objetivos das políticas, papéis e responsabilidades, processos de exceções, abordagem de conformidade, referências a procedimentos, padrões e diretrizes. Sua relevância deve ser regularmente aprovada e ratificada;
- PO6.4 - Distribuição da política - assegurar que as políticas de TIC sejam impostas e distribuídas para todo o pessoal relevante, se consolidando e sendo parte integrante das operações corporativas;
- PO6.5 - Comunicação dos objetivos e diretrizes de TIC - comunicar visando à conscientização e entendimento dos objetivos e direcionamentos de negócios e TIC de todas as partes interessadas e usuários apropriados na organização.



No processo de comunicação se faz necessário identificar quem serão os responsáveis pela geração, coleta, obtenção e análise da informação, também chamado de emissor, bem como para quem será enviada, neste caso o(s) receptor (es) da comunicação (ISACA, 2015; PMI, 2015).

#### **2.7.4. ABORDAGEM CMMI**

Em relação à metodologia CMMI, PERSSE (2007) cita às normas da família ISO, a NBR ISO 10006 para definir os processos relacionados com a comunicação dos projetos (PERSSE, 2007):

- Planejamento da comunicação – considera as necessidades do projeto e dos indivíduos envolvidos, definindo as informações que serão formalmente comunicadas, a frequência e os meios de transmissão utilizados;
- Gerenciamento da informação - inclui procedimentos para preparo, coleta, identificação, classificação, distribuição, preenchimento, atualização, arquivamento e recuperação de informações;
- Controle da comunicação - o sistema de comunicação deve ser implementado como planejado, supervisionado e analisado criticamente, para garantir que continua a atender as necessidades do projeto.

### 3 SURVEY: GOVERNANÇA E ALINHAMENTO ESTRATÉGICO DE TIC E NEGÓCIO

---

Esta seção tem por finalidade apresentar as etapas referentes à montagem e aplicação do *survey*, desde a seleção de participantes, instrumentação, operação, até a análise e interpretação das respostas coletadas.

#### 3.1 PLANEJAMENTO

O objetivo da aplicação do *survey* é identificar o panorama de práticas de Governança de TIC adotadas em empresas sergipanas, do ponto de vista dos CIOs e dos profissionais de TIC. O objetivo é formalizado tendo por base o modelo GQM proposto por Basilli e Weiss (1984): **analisar** a governança de TIC, **com a finalidade** de caracterizar, **com respeito** ao alinhamento estratégico entre TIC e negócio, **do ponto de vista** dos CIOs e profissionais de TIC **no contexto** das empresas sergipanas.

##### 3.1.1. SELEÇÃO DE PARTICIPANTES E TAMANHO DA AMOSTRA

Segundo a CNI (2016), o estado Sergipe possui aproximadamente 3.298 empresas industriais, sendo que 98% delas contam com até 50 empregados e 2% delas têm acima de 250 empregados. Não foram encontradas estatísticas sobre o percentual de indústrias que possuem uma área de TIC formalmente instituída e hierarquizada. É muito provável que boa parte dessas empresas tenha no máximo algum *software* responsável por controles administrativos, financeiros e/ou de produção, ou tenha este serviço terceirizado. A própria estrutura das micro e pequenas empresas não impõe a constituição formal de uma área de TIC. Portanto, a participação dessas empresas iria distorcer as análises, pois as questões não se aplicam ao seu dia a dia. Por isso, a escolha do público-alvo do *survey* teve por princípio entrevistados cujas organizações tivessem uma estrutura definida da área de TIC e que pudessem, em seu dia a dia, executar práticas de Governança, de processos de negócio e de *software*. Por extrapolação, os resultados obtidos a partir desse público podem induzir à compreensão de como as empresas com uma estrutura formal de TIC utilizam práticas estratégicas.

O processo de seleção dos participantes ocorreu por conveniência, cuja população selecionada foi os membros da Associação dos Gestores de Tecnologia da Informação do estado

de Sergipe<sup>3</sup> (CIO-SE) - entidade que congrega os CIOs de várias empresas e de diversos segmentos - e por gestores de TIC de outras empresas do estado.

Apesar da representatividade da amostra só dizer respeito aos profissionais que respondiam pela área de TIC em suas organizações, calculou-se o tamanho da amostra levando em consideração o número de 80 CIOs. O cálculo foi realizado considerando proporções, isto é, percentual da população em relação ao que está sendo avaliado. Como a variância não é conhecida, estima-se a maior variância possível numa proporção de 50% que são favoráveis ao que está sendo avaliado (1/2) e 50% (1/2) desfavoráveis. Logo,  $0,5 \times 0,5 = 0,25$  (variância usada no cálculo). Também foi considerado um nível de significância de 0,05, perfazendo um índice de confiabilidade de 95% e uma margem de erro de 5%. A margem de erro de uma pesquisa aumenta à medida que a população diminui.

Os limites foram alargados considerando e esperando amostras pequenas, encontradas em trabalhos relacionados na área de Engenharia de *Software*. Finalmente, como regra, se feitas 100 pesquisas para o mesmo fim e com a mesma metodologia, em 95 delas os resultados estariam dentro da margem de erro utilizada. Nesse sentido, o valor calculado foi de 67 participantes, estabelecido como meta para o *survey*.

### 3.1.2. METODOLOGIA

A escolha do *survey*, em detrimento de um censo, deveu-se à resistência inicial das pessoas convidadas, de um modo em geral, em participar da pesquisa, mesmo sendo esta relacionada com as necessidades da população.

Foi projetada a execução de um teste piloto com profissionais e gestores de TIC que tivessem uma relação direta com Governança de TIC, planejamento e alinhamento estratégico e processos de *software* na realização das suas tarefas diárias.

Comumente a amostra para esse teste piloto deve ser menor, com fins de identificar possíveis problemas e inconsistências nas perguntas. Esse pré-teste é necessário e visa melhorar o instrumento da pesquisa, sendo executado da mesma forma como será aplicado. A seleção de quem irá participar do pré-teste é flexível, entretanto recomenda-se que as pessoas sejam razoavelmente capacitadas para responder as perguntas (BABBIE, 1999).

A própria constituição da população favoreceu a uma maior diversidade no que se refere ao tipo de organização (pública ou privada), tamanho (pequena, média ou grande) e

---

<sup>3</sup> O CIO-SE tem por objetivos promover capacitações e eventos de inclusão digital e social, incentivar o intercâmbio de informações, organizar, apoiar e divulgar eventos da área de tecnologia da informação e assim fomentar o desenvolvimento da tecnologia da informação do Estado de Sergipe. (<http://www.cio-se.org.br/>).

segmento de atuação. No entanto, essa diversidade não causou obstáculos ao apelo de responder ao *survey*, pois este era destinado aos CIOs.

Alguns cuidados adicionais foram tomados devido à pesquisa ser feita pela *internet* (AAKER *et al.*, 2004): o tempo gasto pelo respondente não deveria ser superior a 10 minutos; o tempo de navegação entre uma página e outra não poderia ultrapassar oito segundos; linguagem clara e abertura em qualquer *browser*.

### 3.1.3. ORGANIZAÇÃO DO QUESTIONÁRIO

As perguntas do *survey* tiveram como referência um questionário aplicado pelo Tribunal de Contas da União (TCU) (TCU, 2015). A opção por utilizá-lo como base foi pautada no fato de que o mesmo possui uma abrangência maior de questões sobre os temas de Governança de TIC e de planejamento e alinhamento estratégico em relação a outros *surveys* encontrados. No entanto, a aplicação na íntegra do *survey* disponibilizado pelo TCU não seria viável devido ao elevado número de questões existentes e pelo tempo que seria necessário para respondê-lo.

Então, a partir dele foram selecionadas inicialmente algumas questões representativas e relacionadas com o objetivo deste trabalho. Dessa forma, o número de questões foi reduzido.

O questionário contém questões de múltipla, única escolha e questões abertas. Ele foi dividido em seis seções, conforme apresentado no Quadro 3.

Quadro 3- Organização do questionário

Seção	Descrição
Identificação do Entrevistado	Questões relativas ao perfil do entrevistado
Identificação da organização	Questões relativas ao tipo e o ramo de atuação da organização.
Estrutura de TIC	Questões relativas aos serviços suportados pela área de TIC e as ferramentas, <i>softwares</i> e sistemas utilizados.
Governança de TIC	Questões relativas às práticas de governança da TIC, sua utilização e vantagens, além de questões relacionadas aos processos organizacionais e de <i>software</i> .
Planejamento e Alinhamento Estratégico	Questões relacionadas à execução do planejamento e alinhamento estratégico de TIC e negócio
Encerramento	Espaço destinado a críticas, comentários e indicação de e-mail para envio dos resultados alcançados.

Fonte: Autor (2017).

Com o intuito de o entrevistado expressar com detalhes sua opinião, utilizou-se a escala *Likert*, a qual permite medir as atitudes e o conhecimento do grau de conformidade do entrevistado diante das questões apresentadas. Nessa escala, as respostas podem ser apropriadas em uma escala ordinal com 3, 5, 7 ou mais categorias a depender do assunto abordado (LAKATOS; MARCONI, 2007).

Foram utilizados dois padrões de respostas baseados na escala *Likert*. O primeiro padrão com opções de resposta "*Discordo plenamente*", "*Discordo parcialmente*", "*Não tenho opinião formada*", "*Concordo parcialmente*" e "*Concordo plenamente*".

As opções no segundo padrão foram: "*Não se aplica*", "*Não adota*", "*Iniciou plano para adotar*", "*Adota parcialmente*" e "*Adota integralmente*". Neste caso, foi adotado um critério gradativo de acordo com o percentual estimado de utilização: 0 – não se aplica; 1 – não adota (0%); 2 – iniciou plano para adotar (>0% e <40%); 3 – adota parcialmente ( $\geq 40\%$  e < 80%), e; 4 – adota integralmente ( $\geq 80\%$ ).

#### **3.1.4. INSTRUMENTAÇÃO**

O questionário (<http://goo.gl/forms/PsWqEjcmoS>) foi desenvolvido na ferramenta *Google Forms* e distribuído por meio da *internet*. Contém uma apresentação inicial, seguido de perguntas referentes à identificação da organização, estrutura de TIC, Governança de TIC, planejamento e alinhamento estratégico de TIC e negócios, identificação do entrevistado e por fim o encerramento.

### **3.2 OPERAÇÃO**

#### **3.2.1. APLICAÇÃO**

Neste momento, a realização da pesquisa foi efetivada. Tudo que fora planejado nas etapas anteriores, então, concretizou-se.

Foi realizada a execução de um teste piloto com alunos do curso de mestrado em Ciência da Computação da Universidade Federal de Sergipe (UFS), gerentes de TIC e coordenadores de informática que tivessem uma relação direta com gestão de processo de negócios, processos de *softwares* e práticas de governança na realização das suas tarefas diárias, selecionados por julgamento e que não participaram da aplicação do *survey*, mas contribuíram para as modificações, tornando o questionário mais claro e objetivo. Nesse piloto, identificou-se

um elevado número de questões, bem como do tempo necessário para respondê-lo (em média 25 minutos). Além disso, alguns itens não se apresentaram com clareza. Os participantes contribuíram com sugestões de melhorias que foram avaliadas, algumas sendo aceitas e incorporadas ao questionário e outras rejeitadas. Após uma revisão das questões, priorizando aquelas que eram objeto do estudo, o questionário foi reformulado e reenviado para nova avaliação. Neste segundo momento, o tempo de resposta foi abaixo dos 10 minutos previstos e não houve qualquer comentário que pudesse suscitar alterações significativas.

Em seguida, os participantes selecionados foram convidados à participação na pesquisa por meio de *e-mails* enviados, bem como por contatos telefônicos e pessoais. Após um mês de convite e disponibilidade do *survey*, entre outubro e novembro de 2015, foram contabilizadas 52 respostas, todas completas e sem nenhuma questão em branco. Apesar dos esforços, contatos pessoais, telefônicos e eletrônicos (*e-mails* e mensagens), não foi possível realizar um censo a fim de atingir toda a população.

### **3.2.2. COLETA E VALIDAÇÃO DE DADOS**

Mesmo tendo sido utilizada uma ferramenta para a construção de *surveys*, foram verificados se os resultados eram realmente coerentes com os apontados por ela, assim como o total de respostas.

Além disso, como forma de validação, foram averiguados os *e-mails* dos participantes, bem como suas respostas, que confirmaram o preenchimento do *survey*.

## **3.3 INTERPRETAÇÃO DOS RESULTADOS**

### **3.3.1. RESULTADOS BRUTOS**

A partir do questionário aplicado buscou-se a compreensão acerca do comportamento das organizações diante do PE e do PE de TIC a partir da análise de métricas como médias, totais e frequências de cada item avaliado.

#### **3.3.1.1. IDENTIFICAÇÃO DO ENTREVISTADO**

A pesquisa foi respondida em sua maioria por Gerentes (37%) e Coordenadores (29%). Apenas 8% ocupavam o cargo na Diretoria. Como o questionário foi enviado para os responsáveis pela área de TIC das organizações, presume-se que em muitas delas as atividades

operacionais, táticas e estratégicas sejam executadas pelas mesmas pessoas. A Tabela 1 demonstra o quadro de resposta do questionário de acordo com a função de cada entrevistado.

Tabela 1- Função dos entrevistados

Função do Entrevistado	Total	(%)
Diretor	4	8%
Gerente	19	37%
Coordenador	15	29%
Supervisor	2	4%
Analista	8	15%
Técnico	2	4%
Outros	2	4%
Total	52	100%

Fonte: Autor (2017).

Do total de entrevistados, 31% alegou que possui certificação ITIL, enquanto 21% registrou possuir a *Certified Scrum Master* (CSM). A Tabela 2 ilustra detalhadamente as certificações dos responsáveis pelas áreas de TIC. Percebe-se claramente que o grupo de certificações da Microsoft é predominante. Dentre os entrevistados, 24 ou 46% não possuem nenhuma certificação. Percebe-se que muitos profissionais possuem mais de uma certificação.

Tabela 2- Certificações dos entrevistados

Certificações	Total	(%) *	(%) **
ITIL - <i>Information Technology Infrastructure Library</i>	16	31%	57%
CSM - <i>Certified Scrum Master</i>	11	21%	39%
MCITP - <i>Microsoft Certified IT Professional</i>	9	17%	32%
MCP - <i>Microsoft Certified Professional</i>	8	15%	29%
MCSA - <i>Microsoft Certified Systems Administrator</i>	6	12%	21%
CCNA - <i>Cisco Certified Technology Specialist</i>	4	8%	14%
COBIT - <i>Control Objectives for Information and Related Technology</i>	4	8%	14%
PMP - <i>Project Management Professional</i>	3	6%	11%
OCA - <i>Oracle Certified Associate</i>	2	4%	7%
MCSE - <i>Microsoft Certified System Engineer</i>	2	4%	7%
SCJP - <i>Sun Certified Java Programmer</i>	1	2%	4%
LPI - <i>Linux Professional Institute</i>	1	2%	4%
Outros	1	2%	4%
Não Possui	24	46%	

Fonte: Autor (2017).

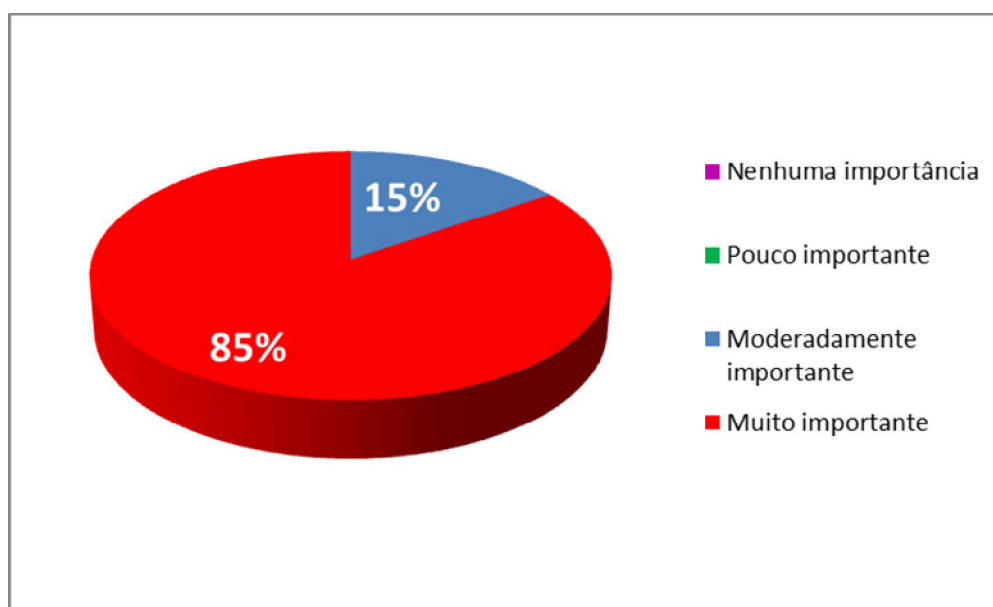
\* - Percentual em relação ao total de entrevistados (52);

\*\* - Percentual em relação ao total de entrevistados que possuem pelo menos uma certificação (28).

O peso da certificação ITIL (57%) se torna mais evidente quando se avalia apenas os entrevistados que possuem pelo menos uma certificação. Essa condição pode se tornar um facilitador dentro das organizações em relação à utilização de boas práticas de Governança de TIC, principalmente no que se refere à gestão dos serviços.

Uma questão importante para o estudo é conhecer a percepção do entrevistado acerca da importância do alinhamento estratégico entre os objetivos do negócio e os objetivos de TIC. Para os entrevistados, 85% acreditam que esse alinhamento é muito importante, seja para a TIC e/ou para o negócio. Os outros 15% acreditam que é moderadamente importante. Vários fatores podem levar a essa percepção, desde a própria cultura organizacional, ao tipo de negócio ou até mesmo a formação profissional de cada uma. O Gráfico 1 ilustra os dados obtidos.

Gráfico 1- Importância do alinhamento estratégico entre TIC e negócio



Fonte: Autor (2017).

### 3.3.1.2. IDENTIFICAÇÃO DA ORGANIZAÇÃO

Pode-se constatar, observando-se a Tabela 3, que há uma distribuição entre os ramos de atuação e segmento das organizações entrevistadas. Isso se deve ao fato de haver várias empresas, de diversos segmentos, que foram contatadas, por meio de seus gestores, para a pesquisa. Saúde, Administração Pública, Comércio, Tecnologia, Educação, Têxtil e Serviços, por exemplo, tiveram maior representatividade.



Tabela 3- Ramo de atuação/segmento da organização

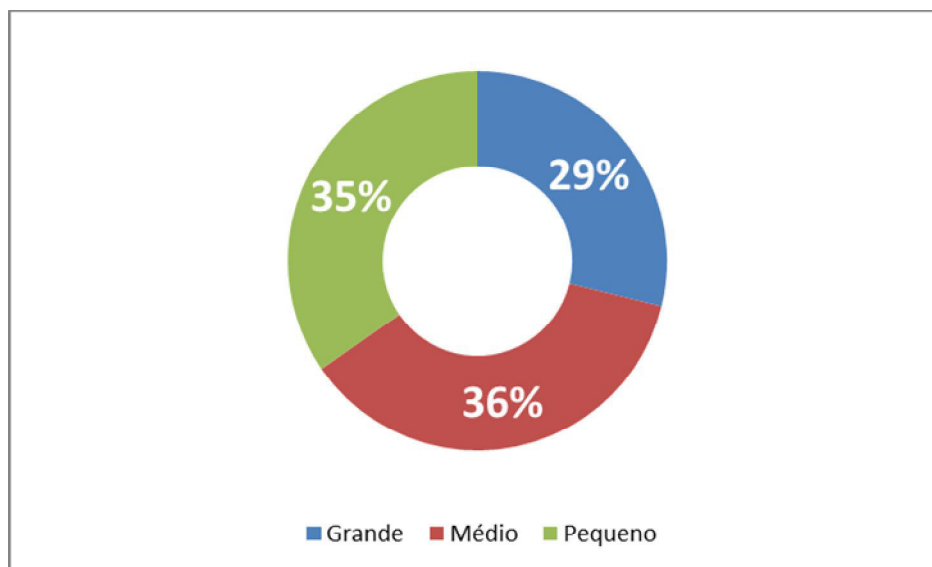
Ramo de atuação/segmento da organização	Total	(%)
Saúde	7	13%
Administração Pública	7	13%
Comércio	6	12%
Tecnologia	5	10%
Educação	5	10%
Têxtil, Vestuário ...	5	10%
Serviços	5	10%
Alimentos e Bebidas	4	8%
Hotéis e Turismo	2	4%
Energia	2	4%
Construção Civil	1	2%
Judiciário	1	2%
Ministério Público	1	2%
Segurança	1	2%
Total	52	100%

Fonte: Autor (2017).

Dos entrevistados, 65% atuam no setor privado e 33% atuam no segmento público e 2% em organizações de economia mista.

Dessas organizações, 35% são de pequeno porte (possuem até 99 funcionários), 36% de porte médio (possuem entre 100 e 499 funcionários) e 29% de grande porte (possuem a partir de 500 funcionários). Esses resultados, apresentados no Gráfico 2, indicam a maior participação das Pequenas e Médias Empresas (PME) na investigação realizada.

Gráfico 2- Tamanho das organizações



Fonte: Autor (2017).

### 3.3.1.3. ESTRUTURA DE TIC

Antes de avaliar a situação do PE da organização e do PE de TIC, bem como o alinhamento entre eles, faz-se necessário buscar o conhecimento da organização e dos serviços executados pela área de TIC.

Como resultado da pesquisa, a área de TIC é responsável principalmente pelos serviços de gestão de infraestrutura (96%), suporte ao usuário (94%), gestão de *hardware* (85%), gestão da segurança da informação (77%), atividades relacionadas com Governança de TIC (77%) e desenvolvimento e manutenção de sistemas (75%). O resultado completo é apresentado na Tabela 4.

Tabela 4- Serviços sob a responsabilidade da gestão de TIC

Serviços sob a responsabilidade da Gestão de TIC	Total	(%)
Gestão de infraestrutura (redes, internet, ativos de rede) e comunicação	50	96%
Suporte ao usuário (computador, impressoras, etc.)	49	94%
Gestão de <i>hardware</i> instalado (compra, substituição, manutenção)	44	85%
Gestão de segurança da informação	40	77%
Governança de TIC (planejamento, melhoria dos processos de TIC, métricas)	40	77%
Desenvolvimento e manutenção de sistemas	39	75%
Serviços de telefonia	36	69%
Gestão de dados (análise de processos e sistemas inteligentes)	31	60%
Gestão de contratos (controle, acompanhamento, contatos, análises)	27	52%
Monitoramento de câmeras	22	42%
Gestão de documentos	19	37%
Gestão de pessoas (treinamento, contratação, ergonomia)	18	35%
Outros	0	0%

Fonte: Autor (2017).

Percebe-se assim a significativa atuação da área de TIC em questões relacionadas à infraestrutura, atendimento ao usuário e a *hardware*, itens de natureza técnica.

Ainda no que tange a utilização de recursos de TIC, a Tabela 5 indica as ferramentas, *softwares* e sistemas de apoio utilizados pelas organizações e que tem participação direta ou indireta da área de TIC, seja como suporte, orientador, prestador do serviço ou apenas como fiscalizador.

Percebe-se claramente a predominância da utilização de Sistemas Informatizados nas organizações: Sistemas de Gestão Integrada (ERP) com 73% e Sistema Legado com 69%. Além disso, a utilização do *Business Intelligence* (BI), 58%, torna-se significativa. Esse resultado

aponta para uma dependência da organização em relação à utilização dos Sistemas Informatizados e para uma busca da organização em ter a sua disposição dados gerenciais e estratégicos para ajuda no processo de tomada de decisão.

Tabela 5- Ferramentas, *softwares* e sistemas de apoio

Ferramentas, <i>softwares</i> e sistemas de apoio utilizados na organização	Total	(%)
Sistemas de gestão integrada (ERP)	38	73%
Sistema legado	36	69%
<i>Business intelligence</i> /Mineração de dados	30	58%
Uso de portal de serviços	28	54%
Sistemas de controle de versões de <i>softwares</i>	26	50%
Sistemas de disparo de <i>e-mails</i>	22	42%
Compartilhamento corporativo (documentos, agenda, etc.)	21	40%
Sistema de relacionamento com clientes (CRM)	18	35%
Uso de mídias sociais ( <i>facebook, linkedIn, twitter, instagram, etc.</i> )	16	31%
Uso de aplicativos para dispositivos móveis	16	31%
Sistema de gerenciamento de documentos (GED/ECM)	15	29%
Sistema de gerenciamento de conteúdo (CMS)	9	17%
Ferramentas para acompanhamento de postagens em redes sociais	6	12%
Ferramentas para otimização de site para mecanismos de buscas	3	6%
Utilização de <i>big data</i>	2	4%

Fonte: Autor (2017).

Outras ferramentas são citadas como utilizadas, mas não é objeto desse estudo identificar o grau de utilização e integração das mesmas. O fato da indicação da utilização de mídias sociais (31%) não significa dizer que esse serviço é mantido atualizado e integrado com os processos organizacionais. Uma tendência representada é a utilização de aplicativos para dispositivos móveis (31%). Isso pode acontecer de diversas maneiras. Seja a recepção de mensagens, consulta a dados e informações do negócio ou até mesmo aplicativos operacionais.

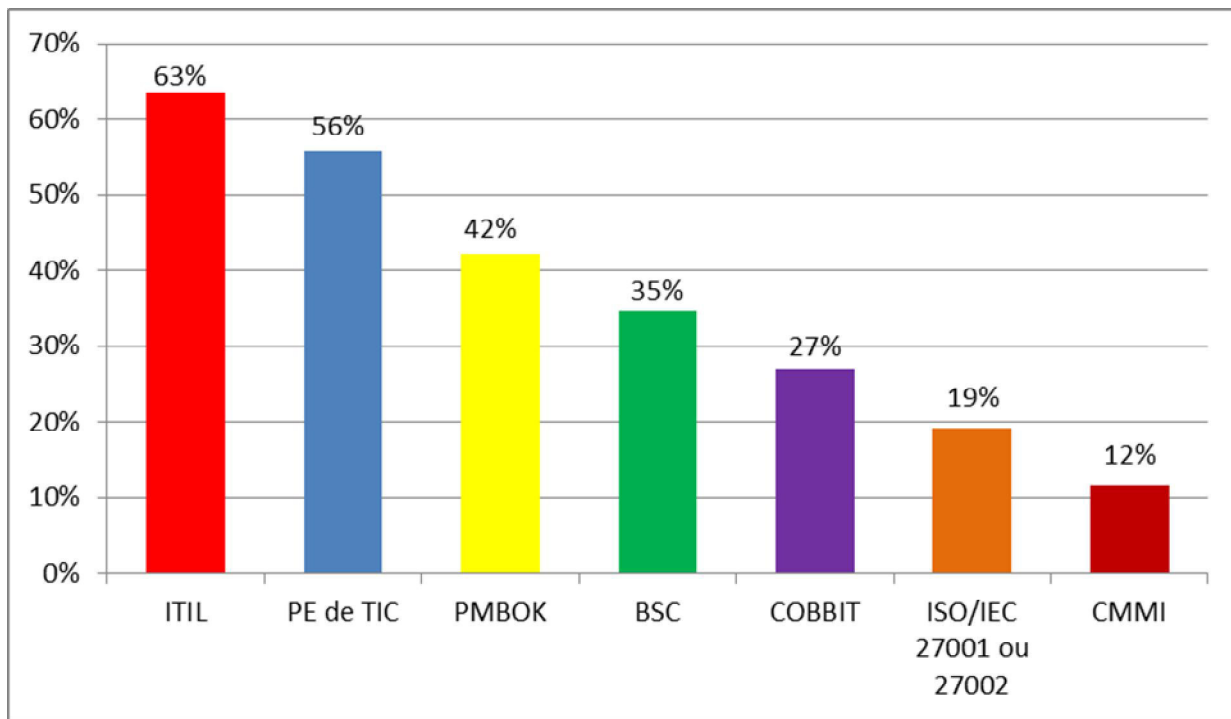
Merece destaque o fato de dois entrevistados, 4%, terem sinalizado a utilização de *Big Data*. Seu grau de utilização não é determinado e também não é objeto deste estudo, no entanto há um esforço no sentido de utilizar esse recurso a favor do negócio.

#### 3.3.1.4. GOVERNANÇA DE TIC

Para garantir e fornecer os serviços de TIC necessários para as organizações e alinhá-los aos objetivos do negócio, práticas de Governança de TIC são utilizadas, seja para permitir a gestão desses serviços, seja para programá-los, monitorá-los e avaliá-los.

Neste caso, as práticas de Governança de TIC mais utilizadas nas empresas de Sergipe são ITIL (63%), PE de TIC personalizado ou criado pela empresa (56%) e PMBOK (42%). O Gráfico 3 contém o resultado completo.

Gráfico 3- Práticas de governança de TIC



Fonte: Autor (2017).

Foi observado que a utilização do PE de TIC pelas organizações sergipanas sinaliza o empenho em procurar alinhar as estratégias de TIC aos objetivos e metas do negócio.

O ITIL também é bastante utilizado e dentre os entrevistados que possuem pelo menos uma certificação, 57% afirmaram ter certificação ITIL. Já a utilização do PMBOK pelas empresas remete a possibilidade de controle dos prazos, dos riscos e de recursos da organização.

As normas de segurança ISO/IEC 27001 ou 27002 com 19% dos dados coletados atestam a pouca preocupação da área de TIC e da organização nas questões de segurança da informação, não apenas de acesso e proteção contra ataques maliciosos, mas principalmente o armazenamento e proteção dos dados.

Um fator de importância que foi observado é que o uso das práticas de Governança de TIC não é excludente, sendo comum a aplicação de mais de uma prática na mesma organização. Isso pode ser observado na Tabela 6, onde são listadas todas as práticas de governança de TIC utilizadas em conjunto.

Tabela 6- Práticas de Governança de TIC utilizadas

Práticas de Governança de TIC utilizadas na organização	(%)
PE de TIC	21%
ITIL, PMBOK	10%
ITIL, BSC	8%
PE de TIC, ITIL, COBIT, CMMI, PMBOK, BSC, ISO/IEC 27001 ou 27002	8%
ITIL	6%
BSC	4%
ITIL, COBIT, PMBOK	4%
PE de TIC, ITIL	4%
PE de TIC, ITIL, COBIT, PMBOK, ISO/IEC 27001 ou 27002	4%
PE de TIC, ITIL, PMBOK	4%
CMMI, ISO/IEC 27001 ou 27002	2%
ITIL, COBIT, BSC	2%
ITIL, COBIT, ISO/IEC 27001 ou 27002	2%
ITIL, COBIT, PMBOK, BSC	2%
PE de TIC, ITIL, BSC	2%
PE de TIC, ITIL, COBIT, CMMI, PMBOK, BSC	2%
PE de TIC, ITIL, COBIT, PMBOK, BSC	2%
PE de TIC, ITIL, COBIT, PMBOK, BSC, ISO/IEC 27001 ou 27002	2%
PE de TIC, ITIL, ISO/IEC 27001 ou 27002	2%
PE de TIC, ITIL, PMBOK, BSC	2%
PE de TIC, PMBOK	2%
PE de TIC, PMBOK, BSC	2%

Fonte: Autor (2017).

Ao se avaliar a utilização das práticas de governança de TIC em relação ao tamanho das organizações, observadas na Tabela 7, percebe-se que o ITIL tem seus conceitos aplicados em 33% das organizações classificadas como pequenas, 19% das médias e 12% das grandes organizações. O fato destas indicarem a utilização do PE de TIC (21%) pode refletir o fato que elas buscam o conjunto de práticas que melhor se adequam à sua realidade.

Tabela 7- Práticas de governança de TIC x tamanho da organização

Prática	Tamanho da Organização			Total
	Grande	Média	Pequena	
ITIL	12%	19%	33%	63%
PE de TIC	21%	23%	12%	56%
PMBOK	12%	12%	19%	42%
BSC	6%	19%	10%	35%
COBIT	10%	12%	6%	27%
ISO/IEC 27001 ou 27002	6%	10%	4%	19%
CMMI	4%	6%	2%	12%
Nenhuma Prática	4%	2%	0%	6%

Fonte: Autor (2017).

A maioria dos entrevistados concordaram parcialmente ou plenamente que as práticas de Governança de TIC reduzem os custos da organização, agilizam a execução dos processos, aumentam a visibilidade sobre o retorno do investimento, aumentam o controle, monitoramento e qualidade dos serviços de TIC, protegem quanto às ameaças, minimizam o impacto da complexidade tecnológica e agregam valor ao negócio.

Tabela 8- Benefícios da utilização de práticas de governança de TIC

A utilização de práticas de Governança de TIC	Discordância		Sem opinião	Concordância	
	Plena	Parcial		Parcial	Plena
Reduz os custos	6%	8%	8%	40%	38%
Agiliza a execução dos processos	4%	2%	8%	40%	47%
Aumenta a visibilidade sobre o retorno do investimento em TIC	0%	2%	4%	19%	75%
Aumenta o controle, monitoramento e qualidade dos serviços de TIC	0%	0%	4%	13%	83%
Protege das ameaças e vulnerabilidade de TIC	2%	2%	8%	42%	46%
Facilita a integração de sistemas e soluções de TIC	0%	2%	29%	35%	35%
Aumenta os lucros	2%	2%	40%	31%	25%
Minimiza o impacto da complexidade tecnológica	2%	2%	17%	40%	38%
Agrega valor ao negócio	0%	0%	15%	13%	71%
Aumenta a competitividade da organização	0%	0%	33%	19%	48%

Fonte: Autor (2017).

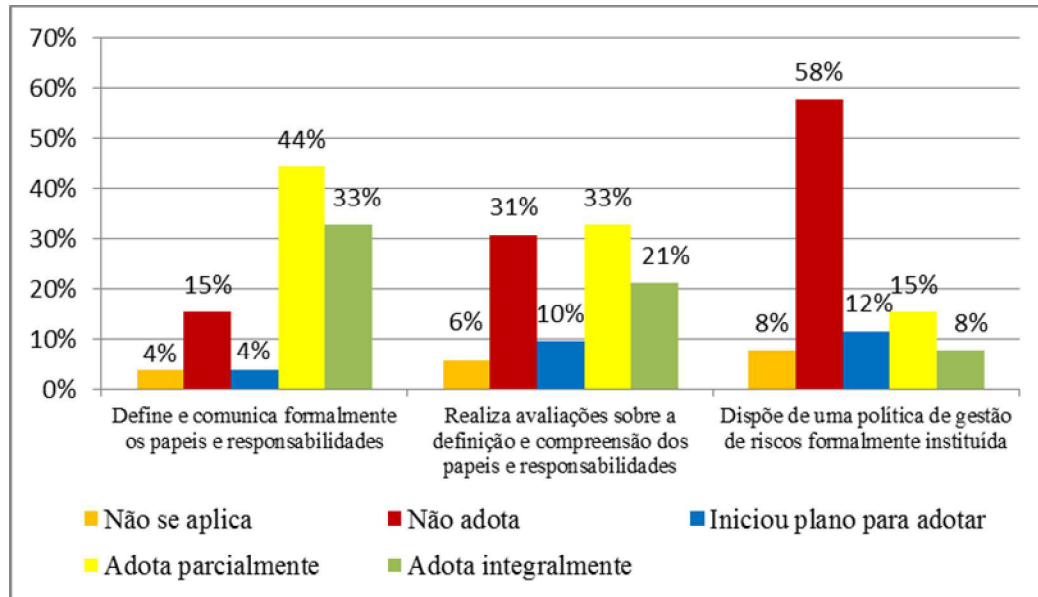
A avaliação quanto ao aumento dos lucros e da competitividade da organização não está bem clara na percepção dos entrevistados. A difusão da perspectiva financeira do BSC (35%) deveria melhorar e esclarecer as vantagens do alinhamento de TIC e negócio, mas isso não é refletido pelas respostas apresentadas. O resultado completo pode ser analisado na Tabela 8.

Em relação ao fato de que as práticas de Governança de TIC agregam valor ao negócio, 84% dos entrevistados concordam parcial ou plenamente. No entanto, é necessário difundir dentro das organizações, por meio de um processo ou plano de comunicação, a geração de valor. Os valores gastos com TIC ainda são elevados, principalmente quando se trata de tecnologia de ponta. A área de TIC e seus recursos não podem ser tratados como custo, mas sim como investimento. Uma aplicação racional de recursos de TIC pode fazer a diferença dentro da organização.

Uma vez analisados os perfis dos entrevistados e da estrutura de serviços da organização, faz-necessário identificar as empresas em relação à Governança e ao seu PE organizacional.

Verificou-se que 33% das organizações adotam a definição formal dos papéis e responsabilidades dos profissionais. Esse resultado merece atenção quando verificado que apenas 21% das organizações realizam avaliações sobre as definições e compreensão dos papéis e responsabilidade dos seus membros, conforme ilustrado no Gráfico 4.

Gráfico 4- Governança na organização: definição dos papéis e gestão de riscos



Fonte: Autor (2017).

A política de gestão de risco requer uma atenção ainda maior, pois apenas 8% das organizações a adota integralmente e 15% adotam parcialmente. Esse resultado é preocupante e faz-se necessário uma atenção especial. O risco faz parte do negócio. Mitigá-lo e conhecê-lo é um diferencial competitivo e de sobrevivência do próprio negócio.

Pode-se afirmar que se o COBIT fosse mais utilizado nas organizações este resultado seria outro, visto que uma de suas premissas é controlar os riscos. O uso do PMBOK pelas organizações deveria minimizar os riscos, pois uma de suas áreas de conhecimento é justamente o gerenciamento de riscos.

Questionados sobre os motivos para não adoção de uma política de gestão de riscos, como ilustrado na Tabela 9, 69% dos entrevistados afirmaram que os riscos são conhecidos por todos e que cada um dos envolvidos sabe o que fazer quando ocorrerem; 62% indicaram que os riscos são considerados eventos normais e do dia a dia; 48% sinalizaram que a causa está na inexistência da cultura de gestão de riscos; 40% indicaram como motivo a burocracia e tempo dedicado; 33% relacionaram a não montagem pelo fato de não ser prioritário; 21% afirmaram que boa parte dos riscos é tratada por outros setores ou prestadores de serviço; e 17% indicaram como motivo a indisponibilidade de pessoal.

Tabela 9- Motivos para não adotar a gestão de riscos

Motivos	Total	(%)
Os riscos são conhecidos por todos e cada um sabe o que fazer quando ocorrerem	36	69%
Os riscos são considerados eventos normais e do dia a dia	32	62%
Inexistência da cultura de gestão de risco	25	48%
A montagem e manutenção são burocráticas e consomem tempo	21	40%
Não é prioritário	17	33%
Boa parte dos riscos é tratada por outros setores ou prestadores de serviços	11	21%
Indisponibilidade de pessoal	9	17%

Fonte: Autor (2017).

Na mesma proporção em que os serviços de TIC são diversos e em grande quantidade, os riscos envolvidos também os são. Neste sentido, buscou-se investigar quais riscos poderiam compor um Plano de Gestão de Riscos de TIC. Detectou-se que 100% dos entrevistados citam a indisponibilidade da *internet*, problemas de armazenamento e *backup* dos dados e informações e indisponibilidade ou falha dos servidores. Problemas no controle de acesso (rede, sistemas, dados, físico) foram citados por 96% dos entrevistados e 92% indicaram as questões relacionadas como utilização de *softwares* não licenciados. A lista completa dos riscos indicados se encontra na Tabela 10.

Tabela 10 - Riscos integrantes de um plano de gestão de riscos de TIC

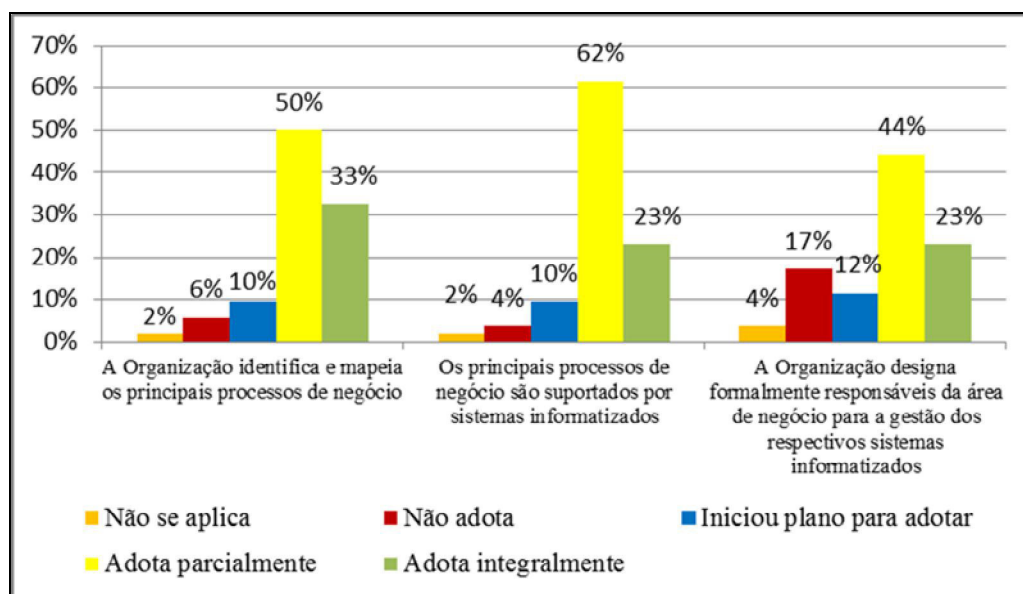
Riscos integrantes de um Plano de Gestão de Riscos de TIC	Total	(%)
Indisponibilidade da <i>Internet</i>	52	100%
Problemas de armazenamento e <i>backup</i> dos dados e informações	52	100%
Indisponibilidade ou falha dos servidores	52	100%
Problemas no controle de acesso (rede, sistemas, dados, físico)	50	96%
Utilização de <i>softwares</i> não licenciados	48	92%
Problemas de telefonia (central telefônica, fixa ou móvel)	40	77%
Falhas na estrutura de rede (física ou sem fio)	38	73%
Falta de energia	30	58%
Falha no desenvolvimento e manutenção do software	28	54%
Problemas no <i>hardware</i> (falta de manutenção, falta de redundância)	25	48%
Proteção contra ataques maliciosos	22	42%
Falha no controle de acesso (físico e lógico)	21	40%
Perda de pessoal	17	33%
Infraestrutura inadequada para atender o negócio	15	29%
Utilização indevida dos sistemas (informações erradas)	13	25%
Vazamento de informações	10	19%
Pessoal não qualificado para as atividades	9	17%
Falta de recursos financeiros	8	15%
Desastres naturais ou atos de vandalismo	5	10%
Incêndios ou inundações	3	6%

Fonte: Autor (2017).



No que se refere à Governança, conforme ilustrado no Gráfico 5, em 33% das empresas, os principais processos da organização são identificados e mapeados e em 50% delas essa prática é adotada parcialmente. Outro ponto importante é a informatização dos processos. Neste caso, 23% dos entrevistados informaram que em suas organizações os processos têm suporte de sistemas informatizados. Para 62% dos entrevistados, esta ação ocorre de forma parcial; 10% deles disseram que a organização irá incluir a informatização no planejamento da empresa. Esse fato possibilita mostrar a existência de uma ampla necessidade de automação dos processos de negócio nas empresas de Sergipe.

Gráfico 5- Governança na organização: processos e informatização



Fonte: Autor (2017).

Ainda se pode observar que em 23% das organizações há a designação formal dos responsáveis das áreas de negócio para a gestão dos sistemas informatizados. Essa conduta pode trazer dificuldades tanto para a organização, sua operação e estratégia, quanto para a própria área de TIC.

Como observado, os processos de negócio são suportados parcial ou integralmente por sistemas informatizados, os quais denotam a gestão do desenvolvimento e manutenção do *software*. Neste sentido, pesquisou-se sobre a gestão do processo de *software*, sendo que em 19% das organizações é adotada integralmente a execução deste processo com objetivo de assegurar que o *software* a ser desenvolvido, direta ou indiretamente, atenda as suas necessidades; e, em 44% essa prática é adotada parcialmente.

As questões descritas na Tabela 11, permitem o entendimento com maior clareza de como se comporta este processo nas organizações. No que se refere ao acompanhamento do

processo por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir, apenas 12% das organizações adotam integralmente e 35% adotam parcialmente, enquanto 15% iniciaram plano para adotar e 23% não adotam essa prática. O processo é periodicamente revisado e melhorado com base nas mensurações obtidas integralmente por apenas 8% das organizações, enquanto 27% o fazem parcialmente e 19% iniciaram plano para adotar. Em 31% das organizações essa prática não é adotada.

Tabela 11- Processo de *software* nas organizações

Processo de <i>Software</i>	Não se aplica	Não adota	Iniciou plano	Adoção	
				Parcial	Integral
A Organização executa processo de <i>software</i> com objetivo de assegurar que o software a ser desenvolvido, direta ou indiretamente, atenda as suas necessidades	15%	13%	8%	44%	19%
O processo de <i>software</i> é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir	15%	23%	15%	35%	12%
O processo de <i>software</i> é periodicamente revisado e melhorado com base nas mensurações obtidas	15%	31%	19%	27%	8%
A Organização possui pessoal próprio capacitado para executar o processo de <i>software</i>	15%	17%	13%	35%	19%
A Organização possui e executa processos de gerenciamento de requisitos	6%	25%	13%	40%	15%
A Organização possui e executa processo de gerenciamento de configuração	6%	29%	13%	40%	12%
A Organização executa processos para garantia da qualidade de processos e produtos	6%	23%	17%	48%	6%
A Organização possui um escritório de projetos, ao menos pra projetos de TIC	6%	67%	4%	17%	6%
A Organização executa processos de testes de <i>software</i>	8%	8%	17%	56%	12%

Fonte: Autor (2017).

No que se refere à organização possuir pessoal próprio capacitado para executar o processo de *software*, isso se faz presente em sua totalidade em 19% das organizações e em 35% delas essa ocorrência é parcial. O processo de gerenciamento de requisitos é adotado integralmente em 15% das organizações e em 40% delas o processo é adotado parcialmente. Iniciaram o plano para adoção 13% das organizações e em 25% delas não há a adoção deste tipo de processo.

O processo de gerenciamento de configuração é executado em 12% das organizações e em 40% há uma adoção parcial. O processo para garantia da qualidade de processos e produtos

é executado em 6% das organizações e em 48% delas há uma prática parcial. O escritório de projetos, ao menos para projetos de TIC, é encontrado em 6% das organizações, enquanto em 17% há uma adoção parcial e 4% iniciaram um plano para adotar. Por outro lado, 67% não possuem esse tipo de escritório. O processo de teste de *software* é executado integralmente em 12% das organizações e em 56% delas há uma adoção parcial, enquanto que em 17% delas há um plano para adotar essa prática.

Em relação às abordagens de Engenharia de *Software*, listadas na Tabela 12, a metodologia orientada a objetos e o desenvolvimento ágil se fazem presentes em 52% das organizações. Prototipação, modelos de ciclo de vida, desenvolvimento iterativo e incremental e reuso são utilizadas respectivamente em 23%, 21%, 21% e 17% das empresas.

Tabela 12- Abordagens de engenharia de *software*

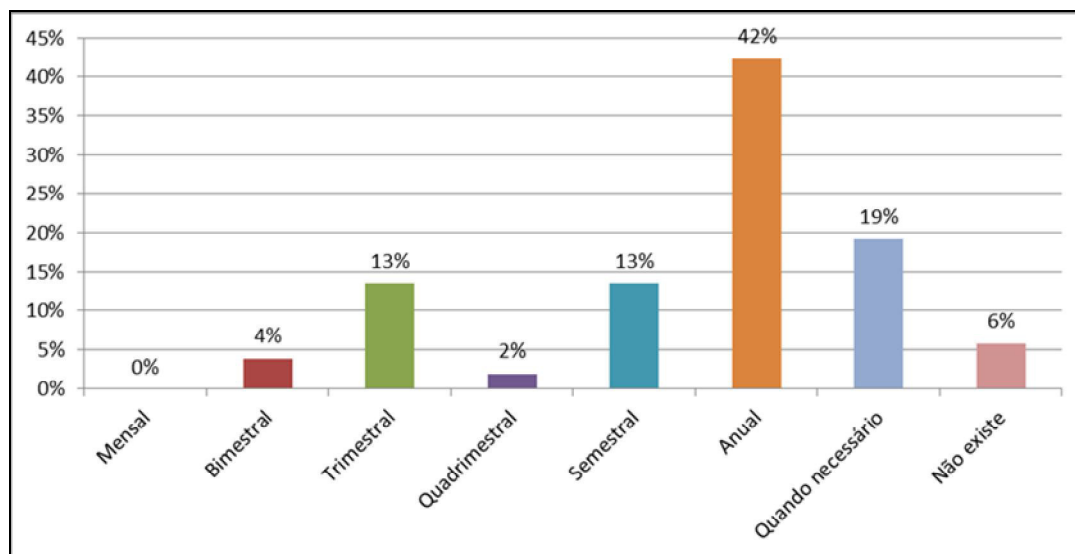
Abordagens de Engenharia de <i>Software</i>	Total	(%)
Metodologia Orientada a Objetos	27	52%
Desenvolvimento Ágil de <i>Software</i>	27	52%
Evolucional ou Prototipação	12	23%
Modelos de Ciclo de Vida	11	21%
Desenvolvimento iterativo e incremental	11	21%
Reuso	9	17%
Modelo Sequencial ou Cascata	4	8%
Espiral	4	8%
Metodologia Estruturada	4	8%
Componentizado	3	6%
V-Model	2	4%
Análise Essencial	2	4%
Outros	1	2%

Fonte: Autor (2017).

### 3.3.1.5. PLANEJAMENTO E ALINHAMENTO ESTRATÉGICO

Conforme apresentado no Gráfico 6, em 42% das organizações o PE é realizado anualmente, em 19% quando necessário e em 13% semestral e trimestralmente. Observa-se que essa periodicidade pode depender do tipo do negócio, bem como do cenário político-econômico vigente. Em algumas organizações, existe a necessidade de se avaliar e revisar seu planejamento em intervalos distintos.

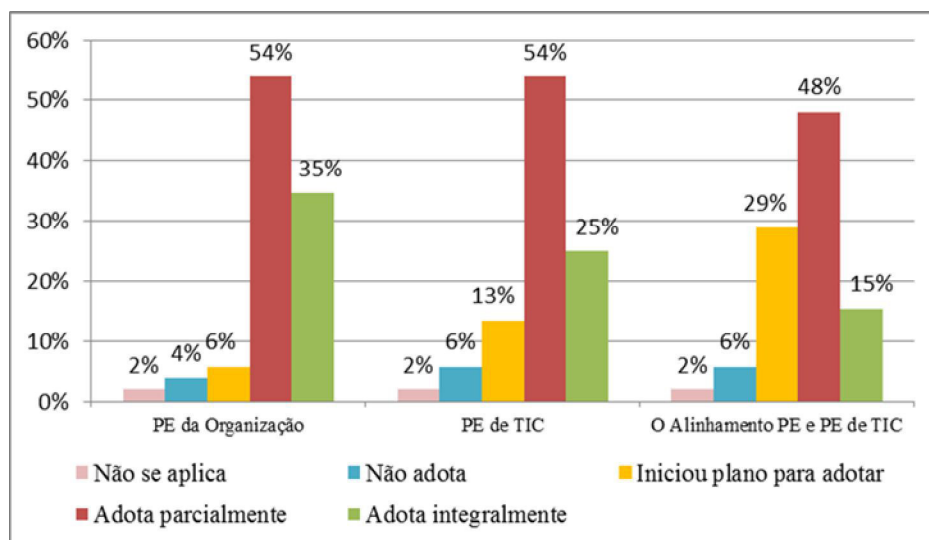
Gráfico 6- Periodicidade do planejamento estratégico na organização



Fonte: Autor (2017).

A aplicação do PE é feita integralmente por 35% das organizações e 54% adotam o PE parcialmente. Em relação ao PE de TIC, o mesmo é adotado integralmente em 25% das organizações e 54% o adotam parcialmente. Já o alinhamento do PE da organização com o PE de TIC é adotado integralmente em 15% das organizações e 48% o adotam parcialmente. O Gráfico 7 apresenta a adoção do PE da organização, do PE de TIC e do alinhamento entre o PE da organização e o PE de TIC.

Gráfico 7- PE da organização, PE de TIC e alinhamento estratégico



Fonte: Autor (2017).

Segundo os entrevistados, 19% afirmaram que o PE de TIC vigente contempla integralmente objetivos, indicadores e metas alinhados aos objetivos de negócio. Outros 52% adotam parcialmente (alinhamento estratégico). Isso pode significar que em curto ou médio prazo um número maior de organizações sergipanas terá alinhamento de TIC e negócio. A Tabela 13 apresenta os questionamentos acerca do PE de TIC nas organizações.

Tabela 13- Planejamento estratégico de TIC

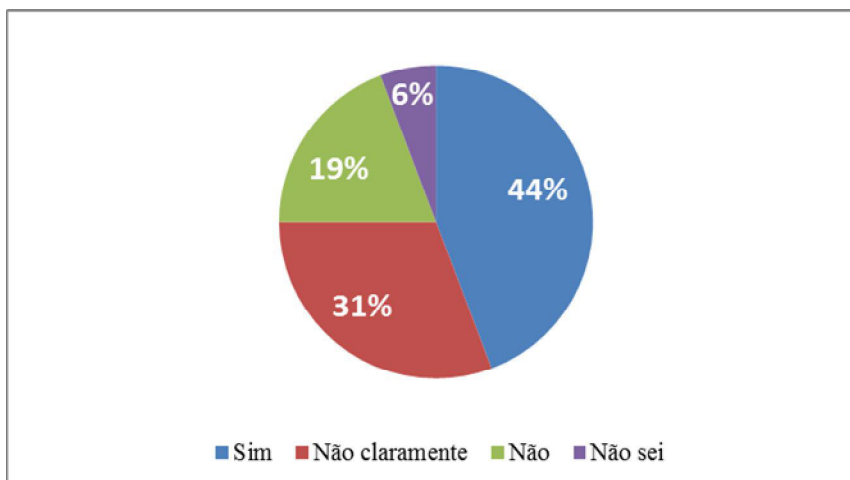
Avaliação do PE de TIC	Não se aplica	Não adota	Iniciou plano	Adoção	
				Parcial	Integral
O PE de TIC vigente contempla objetivos, indicadores e metas de TIC com os objetivos explicitamente alinhados aos objetivos de negócio	2%	8%	19%	52%	19%
O PE de TIC contém alocação de recursos (orçamentários, humanos e materiais) e estratégia de execução indireta (terceirização)	2%	8%	27%	44%	19%
O PE de TIC utiliza métricas que vinculam as ações (atividades e projetos) a indicadores e metas de negócio	2%	27%	23%	38%	10%

Fonte: Autor (2017).

A utilização do PE de TIC com métricas que vinculam as ações (atividades e projetos) a indicadores e metas de negócio foi adotada parcialmente e integralmente por 48% dos entrevistados. No entanto, 27% afirmam não ter adotado qualquer métrica (gestão da mensuração de desempenho). Já no caso do PE de TIC gerenciar a alocação de recursos (orçamentários, humanos e materiais) e estratégia de execução indireta (terceirização), 63% afirmaram que as organizações o fazem parcial ou integralmente.

Um ponto chave para o sucesso do alinhamento estratégico entre PE da organização e o PE de TIC é contar com o apoio da alta direção. Nessa questão, sobre o fato da alta direção ter consciência clara da necessidade desse alinhamento estratégico entre o PE de TIC e negócio, cerca de 44% dos entrevistados afirmaram que sim, mas 31% dos entrevistados declararam que a alta direção não tem consciência clara desta necessidade. Dessa forma, não é possível concluir o quanto importante para a direção da empresa é o alinhamento entre o PE da organização e o PE da TIC (ver Gráfico 8).

Gráfico 8- Consciência da alta direção sobre a importância do alinhamento estratégico



Fonte: Autor (2017).

Uma ação para promover o esclarecimento sobre a importância da TIC para o negócio e os benefícios obtidos com o alinhamento entre as estratégias de TIC e do negócio é estabelecer um plano de comunicação e transparência capaz de expor as atividades de TIC no âmbito interno ou, quando for o caso, no âmbito externo. Segundo 100% dos entrevistados a TIC deve comunicar a disponibilidade e indisponibilidade dos seus serviços, bem como manutenções e atualizações dos *softwares*. Para 92%, é importante que os indicadores e metas de TIC sejam publicados periodicamente e 87% registraram a importância de informar sobre o Catálogo de Produtos e Serviços de TIC. A Tabela 14 contempla a relação completa dos itens indicados pelos entrevistados. O item *Outros* (10%) é composto por: motivos de não atendimento dos chamados, movimentação do quadro de pessoal, uso indevido dos recursos de TIC, boletins informativos sobre tecnologias aplicadas no negócio, escala de trabalho/equipe de sobreaviso.

Tabela 14 - Comunicação e transparência de TIC

Comunicação e Transparência de TIC	Total	(%)
Disponibilidade e indisponibilidade dos serviços de TIC	52	100%
Manutenção e atualização dos <i>softwares</i>	52	100%
Indicadores de resultado da TIC	48	92%
Catálogo de produtos e serviços de TIC	45	87%
Política de segurança da informação	37	71%
Andamento dos projetos de TIC	35	67%
Missão, visão e objetivos da TIC	20	38%
Papéis e responsabilidades da equipe de TIC	9	17%
Gastos e investimentos em TIC	5	10%
Outros	5	10%

Fonte: Autor (2017).

As principais vantagens estabelecidas pelo alinhamento do PE da organização com o PE de TIC são apontadas na pesquisa em visibilidade do valor agregado de TIC nos negócios (88%), visibilidade do papel de TIC (87%), melhor alocação de recursos em TIC (83%) e aprimoramento na execução das estratégias de TIC (71%). O resultado completo é apresentado na Tabela 15.

Tabela 15- Vantagens do alinhamento do PE da organização e o PE de TIC

Vantagens	Total	(%)
Visibilidade do valor agregado de TIC nos negócios	46	88%
Visibilidade do papel da TIC	45	87%
Melhor alocação de recursos em TIC	43	83%
Aumento da performance dos recursos de TIC	37	71%
Aprimoramento na execução das estratégias de TIC	37	71%
Aumento da performance da Organização	24	46%
Aumento das vantagens competitivas	23	44%
Aumento na velocidade de inovação	16	31%
Não há vantagens	0	0%
Outras	0	0%

Fonte: Autor (2017).

A respeito das dificuldades para a implementação do PE de TIC nas organizações, observadas por completo na Tabela 16, identificou-se que a principal (77% dos casos) é a não cooperação das áreas envolvidas. Dos entrevistados, 48% afirmaram que o PE de TIC não é prioridade e 48% afirmaram que falta comprometimento da alta direção. O resultado encontrado está relacionado com o fato de que 31% dos entrevistados afirmaram que, para a alta direção, não está clara a necessidade do alinhamento de TIC e negócio e 19% afirmaram que a alta direção não tem consciência dessa importância. O apoio da alta direção é fator crucial para a implantação do alinhamento estratégico.

Tabela 16- Dificuldades para implantação do PE de TIC

Dificuldades para a implementação/manutenção do PE de TIC	Total	(%)
Não cooperação das áreas envolvidas	40	77%
Falta de comprometimento da Alta Direção	25	48%
Não é prioritário	25	48%
Falta de tempo	24	46%
Falta de conhecimento de como fazer	10	19%
Não há dificuldades	1	2%
Outras	1	2%

Fonte: Autor (2017).

### 3.3.2. AMEAÇAS À VALIDADE

Embora os resultados da pesquisa tenham se mostrado satisfatórios, a mesma apresenta ameaças à sua validade que não podem ser desconsideradas e diferentes problemas podem ser ocasionados durante a participação dos indivíduos no questionário:

- **Ameaças à validade interna** - instrumentação adequadamente preparada – os participantes responderam ao questionário sem nenhuma supervisão, assim, há a probabilidade dos mesmos não terem entendido alguma questão específica. A realização do piloto foi contemplada justamente para mitigar esse tipo de problema.
- **Ameaças à validade externa** - representatividade da população – a variedade dos participantes que responderam ao questionário foi significativa, cerca de 65% da população, no entanto abaixo do valor mínimo calculado para o tamanho da amostra. Estima-se que resultado semelhante seja obtido aplicando a pesquisa em outros grupos devido às características da população. O fato de utilizar-se o *survey* por meio de um questionário disponibilizado na *internet* não garante que quem respondeu tenha sido realmente o gestor, mas sim alguém indicado por ele.
- **Ameaças à validade de conclusão** - distribuição do conjunto de participantes – as funções ou cargos dos participantes podem afetar os resultados, entretanto, a maioria das respostas foi obtida por cargos de chefia. Há o risco das respostas serem verdadeiras, porém não condizentes com a prática, como por exemplo, afirmar a existência de um plano ou procedimento, o qual existe formalmente no papel, porém na prática a empresa não o executa.

## 3.4 CONSIDERAÇÕES FINAIS DO CAPÍTULO

De uma forma geral, conforme o resultado da pesquisa, as empresas de Sergipe adotam (parcial ou integralmente) ou iniciaram ações para adotar o PE da organização, o PE de TIC e o alinhamento do PE da organização e o PE de TIC. Isso é um sinal de que as organizações estão se modernizando e passando a planejar suas ações.

Pelos resultados obtidos percebe-se que apenas em 44% das organizações a alta direção tem consciência clara da importância da necessidade do alinhamento estratégico de TIC e negócio. Esse resultado pode implicar diretamente na execução do PE e do PE de TIC e no alinhamento entre ambos. Para tentar esclarecer ou dirimir quaisquer dúvidas é necessário



executar estratégias de comunicação eficazes e, neste caso, deve-se manter a alta direção ciente dos acontecimentos relativos à área de TIC, informar sobre os projetos existentes, compartilhar e socializar o conhecimento e ainda associar a informação a processos operacionais, ressaltando a importância da TIC para a organização.

Atesta-se que as empresas de Sergipe adotam prioritariamente o ITIL (63%), o PE de TIC próprio ou personalizado (56%) e PMBOK (42%). Essas práticas, na maioria das vezes, são utilizadas em conjunto e sua aplicação depende da natureza do negócio. Neste caso, os resultados corroboram a importância dada, pelas organizações, ao PE e ao PE de TIC. Essas práticas de Governança irão orientar como a área de TIC poderá alcançar suas metas.

## 4 PROPOSTA DE MELHORIAS NA METODOLOGIA PETIC

---

Esta seção apresenta a proposta da dissertação em incorporar melhorias à Metodologia PETIC, maximizando sua aplicação e benefícios dentro da organização, ampliando seu escopo com a inclusão da gestão de riscos e a da comunicação e transparência de TIC a partir da revisão da literatura e da análise do *survey* sobre a adoção das práticas de Governança de TIC no âmbito das empresas sergipanas, apresentado na seção 3.

Inicialmente será descrita a proposta de inclusão da gestão de riscos de TIC com a montagem do catálogo dos riscos de TIC, dos gráficos utilizados para análises e decisões e do plano de respostas aos riscos.

Em um segundo momento será apresentado o plano de comunicação e transparência de TIC, responsável pelo gerenciamento da informação.

Em seguida, para comportar a introdução da gestão de riscos e da comunicação e transparência de TIC, são sugeridas e descritas as alterações no *workflow* e nos componentes da Metodologia PETIC.

Por fim, será apresentado o resumo do que foi exposto na seção.

### 4.1 GESTÃO DE RISCOS DE TIC

A análise dos dados obtidos com a realização do *survey*, apresentado na seção 3, indicou que a adoção de uma política formal de gestão de riscos de TIC existe em apenas 8% das organizações pesquisadas. Dada à importância do tema, é um resultado significativamente baixo e preocupante e que pode comprometer o atendimento das metas e objetivos de TIC e da organização.

Como fatores para a não adoção formal de um plano de gestão de riscos de TIC, 69% dos entrevistados indicam que os riscos são conhecidos por todos e que cada um dos envolvidos sabe o que fazer quando ocorrerem. Outros 62% indicam que os riscos são considerados eventos normais e do dia a dia e 48% indicam a inexistência da cultura da gestão de riscos. Chama a atenção o fato de 40% dos entrevistados sinalizarem que a montagem de um plano de gestão de riscos é uma atividade burocrática e que consome tempo.

Percebe-se, com esses números, que incorporando um modelo simples ao processo de elaboração do PE de TIC haverá a possibilidade de implantar uma gestão de riscos de TIC eficaz

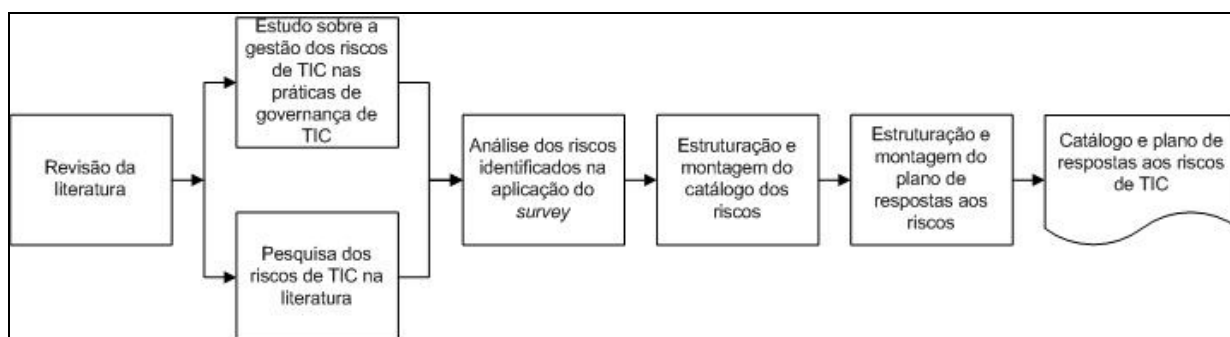
e que seja benéfica para as estratégias e operação da área de TIC, impondo um aspecto formal a um acompanhamento que já é feito informalmente e não sistemático no dia a dia.

#### 4.1.1. ELABORAÇÃO DA PROPOSTA DA GESTÃO DE RISCOS DE TIC

Esta dissertação propõe a incorporação da gestão de riscos de TIC na Metodologia PETIC de modo que seja possível ao gestor além de definir e acompanhar as estratégias de TIC, ter conhecimento de potenciais eventos que inviabilizem o atingimento das suas metas e objetivos, bem como a execução das estratégias necessárias ao negócio.

A estruturação da gestão de riscos de TIC, ilustrada na Figura 8, foi montada empiricamente, baseada na aplicação de técnicas de Gerenciamento dos Riscos em diversos projetos com participação do autor, utilizando como referência a literatura sobre os processos de gerenciamento de riscos dos modelos e *frameworks* das boas práticas de Governança de TIC como ITIL, PMBOK, COBIT, CMMI e ISO27005 e a análise do *survey* objeto deste trabalho.

Figura 8 - Fluxo da elaboração da proposta da gestão de riscos de TIC



Fonte: Autor (2017).

A partir da revisão da literatura, a biblioteca ITIL foi utilizada como base para dar suporte à continuidade ao negócio e procedimentos para que os serviços possam ser recuperados dentro de prazos acordados; o PMBOK forneceu a base para o gerenciamento dos riscos; os processos do COBIT permitiram o entendimento das questões de Governança de TIC e o impacto no negócio; o CMMI tratou dos aspectos relativos aos processos de Engenharia de *Software*; e a ISO 27005 tratou das questões de segurança da informação. Além disso, o Catálogo de Processos de TIC da Metodologia PETIC forneceu os processos para a associação dos riscos. Também foram identificados riscos de TIC listados por diversos autores.

A seguir serão apresentadas a estruturação do catálogo de riscos, da montagem dos gráficos e do plano de respostas aos riscos de TIC.

#### 4.1.2. CATÁLOGO DOS RISCOS DE TIC

O Catálogo dos Riscos de TIC é o repositório onde os riscos estarão relacionados e associados aos processos existentes no Catálogo de Processos de TIC da Metodologia PETIC para realização das análises qualitativas, quantitativas e para priorização e identificação do tratamento a ser dado a cada um deles.

Os atributos do Catálogo dos Riscos foram determinados a partir da revisão da literatura e são apresentados no Quadro 4, onde também são observadas a utilização de cada um deles em relação nas práticas de governança de TIC estudadas.

Quadro 4 - Atributos do catálogo dos riscos de TIC

Atributo	Fonte / Origem					
	ITIL	PMBOK	COBIT	CMMI	ISO	PETIC
Identificador, nome e descrição do risco.	X	X	X	X	X	
Categoria do risco quanto às áreas: dados, <i>hardware</i> , <i>software</i> ; telecomunicação, pessoas e governança de TIC.						X
Processo associado ao risco.						X
Avaliação qualitativa do risco quanto à probabilidade impacto no negócio: muito baixa, baixa, média, alta ou muito alta.	X	X	X	X	X	
Avaliação quantitativa do risco quanto ao impacto financeiro na ocorrência dos riscos.	X	X	X		X	
Classificação do risco quanto à prioridade para ser gerenciado.	X	X	X	X	X	
Identificação do tratamento diante da avaliação do risco: evitar, mitigar, transferir ou assumir.	X	X	X	X	X	

Fonte: Autor (2017) baseado na revisão da literatura.

O Catálogo dos Riscos de TIC, mostrado no Apêndice A, está preenchido com 79 riscos de TIC oriundos da revisão da literatura e da análise e redefinição dos 20 riscos identificados na análise do *survey*, Tabela 10 da seção 3. Cada um dos riscos está associado a um processo da Metodologia PETIC.

A partir do Catálogo dos Riscos de TIC proposto, o gestor poderá excluir riscos que não correspondem à realidade da organização ou incluir outros que fazem parte do negócio. Como resultado, ter-se-á o Catálogo atualizado e contendo todos os riscos de TIC da organização,

os quais devem ser avaliados qualitativa e quantitativamente, terem suas prioridades definidas, bem como o tratamento a ser dado aos riscos.

O Quadro 5 exemplifica o preenchimento dos atributos de um risco identificado no Catálogo dos Riscos de TIC.

Quadro 5 - Exemplo do catálogo dos riscos de TIC

Atributo	Valor
Identificador do risco	7.1
Descrição do risco	<i>Falha na instalação, configuração ou administração do BD.</i>
Categoria do risco	<i>Dados</i>
Processo associado ao risco	<i>1.1.1 - Administração do Banco de Dados</i>
Probabilidade de ocorrência do risco	<i>Alta (80%)</i>
Impacto da ocorrência do risco	<i>Muito Alta (90%)</i>
Impacto Financeiro do risco	<i>100000</i>
Valor Médio Esperado (VME)	<i>8000</i>
Classificação do risco quanto ao grau de prioridade	<i>Alto</i>
Identificação do tratamento do risco	<i>Evitar</i>

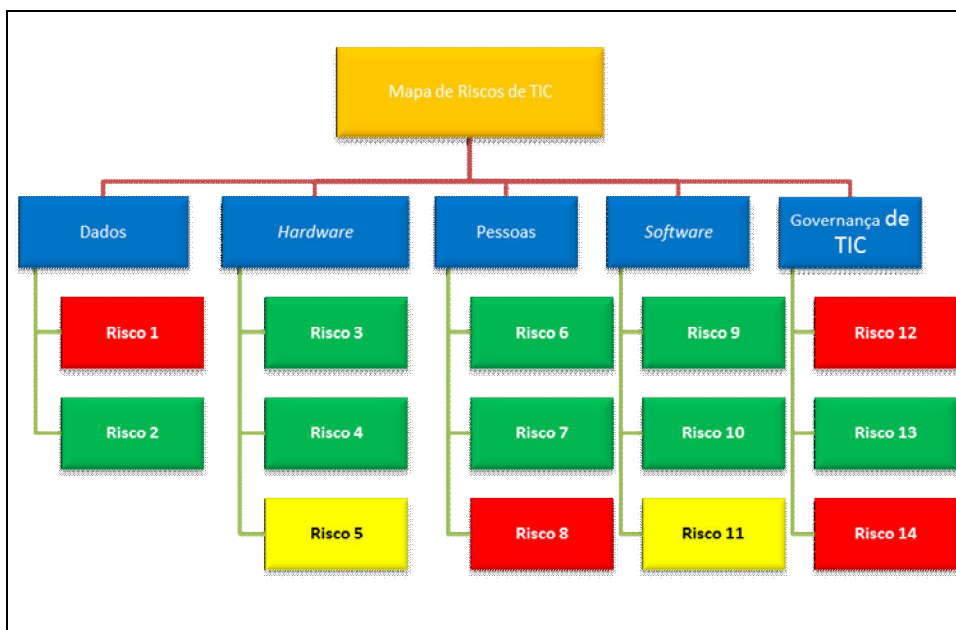
Fonte: Autor (2017).

#### 4.1.3. GRÁFICOS PARA ANÁLISE DOS RISCOS DE TIC

O Mapa dos Riscos de TIC e o Gráfico de Impacto x Custos dos Riscos são os gráficos propostos para auxiliar na análise dos riscos e no processo de tomada de decisões.

A representação gráfica do Mapa dos Riscos de TIC, observada hipoteticamente na Figura 9, segue a mesma estrutura existente no PMBOK em relação à Estrutura Analítica do Projeto (EAP). Contém os riscos de TIC priorizados e agrupados por categoria (dados, *hardware*, pessoas, *software*, telecomunicações e Governança de TIC), possibilitando uma visualização mais efetiva dos riscos avaliados e priorizados.

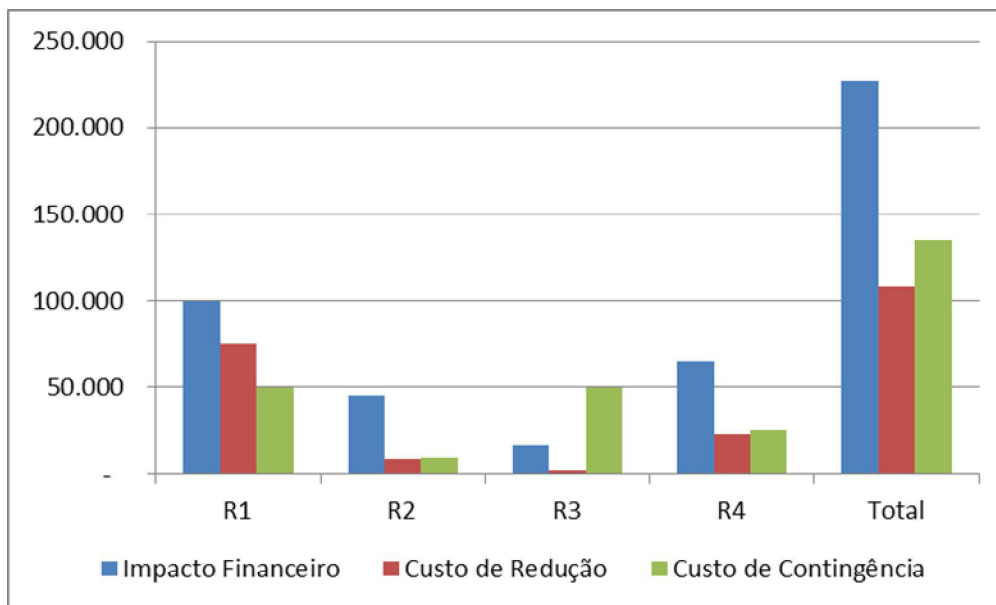
Figura 9- Mapa dos riscos de TIC



Fonte: Adaptado de PMI (2015).

O Gráfico de Impacto x Custos dos Riscos de TIC, ilustrado na Gráfico 9, indica o impacto financeiro em caso de ocorrência, o custo para redução e o custo de contingência do risco.

Gráfico 9- Gráfico de impacto x custos dos riscos de TIC



Fonte: Autor (2017).

#### 4.1.4. PLANO DE RESPOSTAS AOS RISCOS DE TIC

O Plano de Respostas aos Riscos de TIC representa o conjunto de ações que devem ser executadas para evitar, mitigar, assumir ou transferir os riscos, além de conter as ações para contingenciamento. Trata-se do que fazer, quando e como fazer para evitar ou mitigar o risco ou após a sua ocorrência.

Assim como a avaliação, priorização e tratamento dos riscos variam por organização e suas especificidades, a resposta ao risco de TIC dependerá da estrutura da TIC, objetivos estratégicos, metas e recursos (*hardware, software, pessoal, financeiro, etc.*).

Os atributos que definem a estrutura do Plano de Respostas aos Riscos de TIC são:

- Identificador, nome e descrição do risco;
- Ações a serem executadas para redução do risco;
- Ações necessárias para contingência do risco;
- Custos para redução e custos para contingência do risco;
- Responsável pela execução da tarefa;
- Prazo para execução da tarefa;
- Partes interessadas ou envolvidas com a ocorrência do risco;
- Status de execução das tarefas.

O Apêndice B apresenta o Plano de Repostas aos Riscos de acordo com o Catálogo dos Riscos de TIC proposto.

## 4.2 GESTÃO DA COMUNICAÇÃO E TRANSPARÊNCIA DE TIC

A análise do *survey*, seção 3, proporcionou a identificação que alguns pontos que atestam a necessidade da área de TIC em proporcionar uma gestão efetiva da comunicação de informações relativas à área.

Para 75% dos entrevistados, a utilização de práticas de governança de TIC aumenta a visibilidade sobre o retorno do investimento em TIC e em apenas 33% das respostas existe a constatação de que a organização define e comunica formalmente os papéis e responsabilidades de cada um. Nestes dois casos percebe-se a necessidade de que haja uma comunicação específica para compartilhar com as demais áreas, seja a aplicação e resultados dos investimentos em TIC ou os papéis e responsabilidades das pessoas.

Outro ponto que chama a atenção é o fato que apenas 44% dos entrevistados indicaram que a alta direção tem consciência da importância do alinhamento estratégico entre

TIC e negócio. Não obstante a falta de uma análise mais profunda acerca dos motivos que impedem uma maior consciência por parte da alta direção, indiscutivelmente que é necessário criar mecanismos para que a alta direção tenha conhecimento das ações, atividades, aplicação e importância da TIC para o negócio.

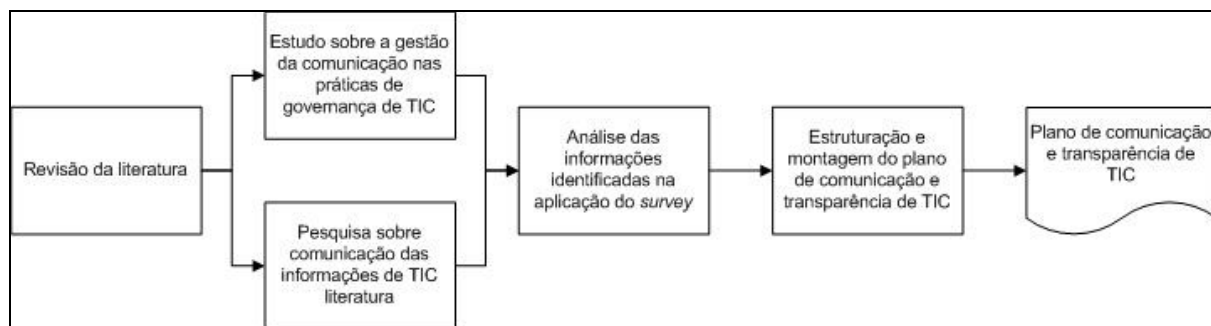
Em muitos casos a falta de consciência pode acontecer pela inexistência de um plano de comunicação de TIC eficiente, que pode inclusive interferir nas dificuldades para implementação do PE de TIC, pois segundo 77% dos entrevistados não há cooperação das áreas envolvidas.

#### 4.2.1. ELABORAÇÃO DA PROPOSTA DO PLANO DE COMUNICAÇÃO E TRANSPARÊNCIA DE TIC

A proposta da incorporação da gestão da comunicação e transparência de TIC na Metodologia PETIC tem por objetivo orientar e detalhar as ações necessárias para disponibilizar as informações da TIC com segurança, integridade, confiabilidade para o local apropriado, no tempo certo, garantindo a tomada de decisões de maneira otimizada, atendendo às necessidades da instituição. Além disso, fornecerá subsídios para corrigir problemas internos de comunicação e que dificulta o dia a dia da área.

A estruturação da gestão da comunicação e transparência de TIC, ilustrada na Figura 10, foi definida empiricamente, a partir da literatura sobre os processos de comunicação dos modelos e *frameworks* das boas práticas de governança de TIC como PMBOK e COBIT, CMMI e ISO27005 e a análise do *survey* objeto deste trabalho.

Figura 10 - Fluxo da elaboração da proposta da gestão de comunicação e transparência de TIC



Fonte: Autor (2017).

O plano de comunicação e transparência de TIC será apresentado a seguir.



#### 4.2.2. PLANO DE COMUNICAÇÃO E TRANSPARÊNCIA DE TIC

O plano de comunicação e transparência de TIC é o repositório que armazena as informações que a área de TIC deve comunicar aos seus clientes internos e externos.

O Quadro 6 apresenta os atributos necessários para estruturação do plano de comunicação e transparência de TIC, montado a partir da revisão da literatura.

Quadro 6 - Atributos do plano de comunicação e transparência de TIC

Atributo	Fonte / Origem					
	ITIL	PMBOK	COBIT	CMMI	ISO	PETIC
Identificação e descrição da informação	X	X	X	X		
Classificação da informação		X	X			
Responsável por obter e emitir informação		X	X			
Formato e <i>layout</i> da informação						
Partes interessadas ou destinatários da informação	X	X	X	X		
Meio de comunicação para envio da informação		X	X			
Periodicidade que deve ser enviada a informação		X	X			
Período de vigência que a informação deve ser enviada		X	X			
Procedimentos para descarte e arquivamento das informações enviadas						

Fonte: Autor (2017) baseado na revisão da literatura.

O plano de comunicação e transparência de TIC, mostrado no Apêndice C, está preenchido com 15 informações oriundas da revisão da literatura e da análise do *survey*, Tabela 14 da seção 3.

A partir deste plano, o gestor poderá excluir as informações que não correspondem à realidade da organização ou incluir outras que fazem parte do negócio. Como resultado, ter-se-á o plano contendo todas as informações de TIC da organização que devem ser compartilhadas de acordo com a classificação da informação e as partes interessadas.

Abaixo, o Quadro 7 exemplifica o preenchimento dos atributos do plano de comunicação e transparência de TIC.

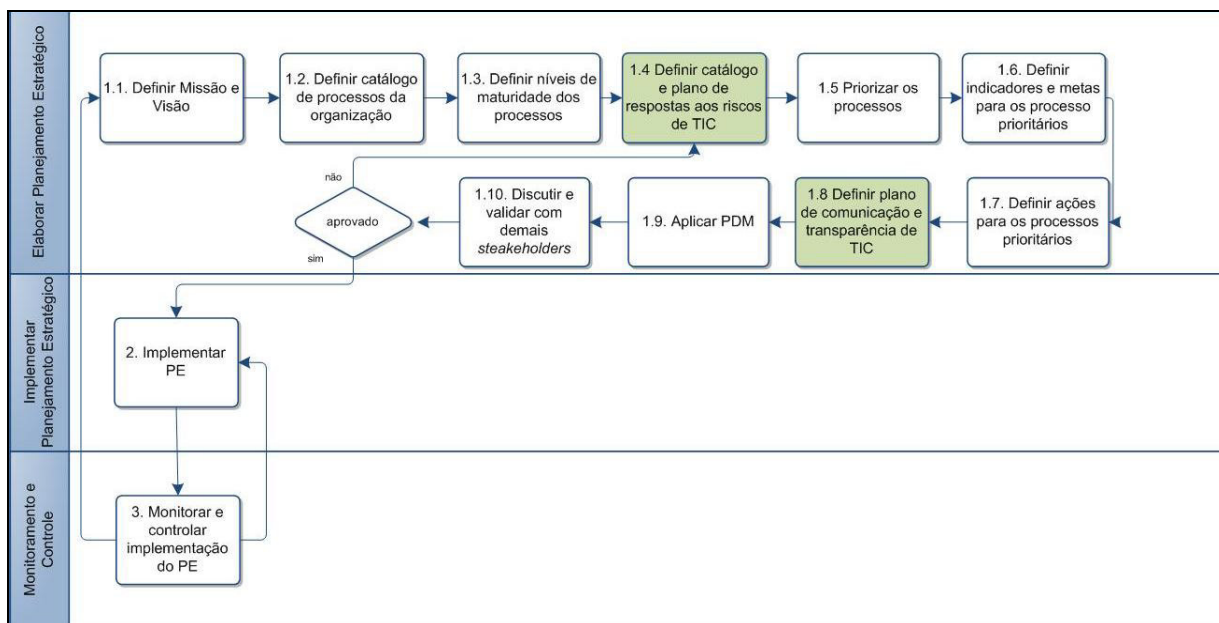
Quadro 7 - Exemplo do plano de comunicação e transparência de TIC

Atributo	Valor
Identificação	8.1
Descrição da informação	<i>Resultados periódicos dos indicadores de TIC</i>
Classificação da informação	<i>Uso interno</i>
Responsável por obter e emitir informação	<i>Gerente de TIC</i>
Formato e <i>layout</i> da informação	<i>Utilizar formato padrão da empresa para apresentação dos indicadores de resultado</i>
Partes interessadas ou destinatários da informação	<i>Todos os departamentos da organização</i>
Meio de comunicação para envio da informação	<i>e-mail</i>
Periodicidade que deve ser enviada a informação	<i>Mensal (até o 5º dia do mês subsequente)</i>
Período de vigência que a informação deve ser enviada	<i>Permanente</i>
Procedimentos para descarte e arquivamento das informações	<i>A informação deve ser arquivada mensalmente, bem como se deve manter o seu histórico anual</i>

Fonte: Autor (2017).

### 4.3 PROPOSTA DE ALTERAÇÃO NO WORKFLOW DA METODOLOGIA PETIC

O *workflow* da Metodologia PETIC deve ser alterado para incorporar a gestão de riscos e da comunicação e transparência de TIC apresentadas anteriormente. Propõe-se, como ilustrado na Figura 11, a inclusão de etapas de *elaboração do plano de identificação, priorização e respostas aos riscos de TIC* e *elaboração do plano de comunicação e transparência de TIC*.

Figura 11 - Proposta de alteração do *workflow* PETIC

Fonte: Adaptado de Rocha (2017)

A inclusão da definição do catálogo e do plano de respostas aos riscos de TIC corresponderá à fase da PETIC responsável pela gestão de riscos e é dividida nas seguintes fases:

1. Análise e atualização do catálogo dos riscos de TIC;
2. Avaliação qualitativa e quantitativa dos riscos;
3. Priorização dos riscos;
4. Análise gráfica: mapa dos riscos de TIC e gráfico de impacto x custos dos Riscos de TIC;
5. Estruturação do plano de respostas aos riscos priorizados.

Para definição do plano de comunicação e transparência de TIC é necessário que durante a realização do PE de TIC as fases abaixo sejam realizadas:

1. Identificação, definição do conteúdo, classificação, responsáveis e partes interessadas nas informações que devem ser comunicadas;
2. Estruturação do planejamento (meios de comunicação, periodicidade, vigência e descarte da informação) da comunicação da informação.

Como resultado, propõe-se também a inclusão de novos componentes na Metodologia PETIC, como ilustrado e destacado na Figura 12, a saber: a) Catálogo dos riscos de TIC; b) Mapa dos riscos de TIC; c) Gráfico do impacto x custo dos riscos de TIC; d) Plano de respostas aos riscos, e; e) Plano de comunicação e transparência de TIC.

Figura 12 - Proposta de novos componentes na Metodologia PETIC

P E T I C	Catálogo de Processos de TIC	
	Repositório de Ações	
	Catálogo de Ferramentas e Técnicas	
	Catálogo dos Riscos de TIC ★	
	Mapa dos Riscos de TIC ★	
	Gráfico do Impacto x Custos dos Riscos de TIC ★	
	Plano de Resposta aos Riscos de TIC ★	
	Plano de Comunicação e Transparência de TIC ★	
	Artefato PETIC	
	Gráficos de Importância	Mapas de Gantt

Fonte: Adaptada de Palmeira (2012)

#### 4.4 CONSIDERAÇÕES FINAIS DO CAPÍTULO

As propostas aqui apresentadas visam dotar a Metodologia PETIC de mecanismos para a gestão de riscos e da comunicação e transparência de TIC.

No que se refere à gestão de riscos de TIC é sugerido um catálogo de riscos, estruturado a partir de metodologias, *frameworks* e boas práticas de governança de TIC (ITIL, COBIT, ISO-9000, PMBOK e CMMI) e contendo alguns riscos pré-selecionados a partir da revisão da literatura e do *survey*, parte integrante desta dissertação. A lista de riscos pré-definida deve ser analisada durante a elaboração do PE de TIC e adequada à realidade da organização, resultando assim em um catálogo de riscos de TIC da organização. O catálogo atualizado deve ser avaliado e priorizado, gerando o mapa de riscos de TIC e o gráfico do impacto x custos dos riscos. Posteriormente é mantido o plano de respostas aos riscos, contendo as ações de redução e contingenciamento dos riscos.

Já no caso da comunicação e transparência de TIC nota-se que o COBIT e o PMBOK se destacam mais em relação a esse tema. Por esse motivo, dedicar atividades para gerenciar a comunicação e transparência de TIC na Metodologia PETIC se justifica pelo fato da comunicação representar um dos pilares da Governança. Também se buscou na literatura e na análise do *survey* uma lista pré-definida de informações associadas à área de TIC e que podem representar um aumento da transparência das ações de TIC. A partir da análise desta lista, poder-se-á montar o plano de comunicação e transparência da organização, atendendo suas prioridades e estratégias de negócio.

Como resultado, propõe-se a inclusão de novos componentes na Metodologia PETIC:

a) Catálogo dos riscos de TIC; b) Mapa dos riscos de TIC; c) Gráfico do impacto x custo dos riscos de TIC; d) Plano de respostas aos riscos, e; e) Plano de comunicação e transparência de TIC.

O princípio básico para estruturação dessas melhorias foi a simplicidade e a praticidade. As diversas metodologias, *frameworks* e práticas dispõem de vários procedimentos, alternativas, fluxos e processos para tratarem a gestão do risco e gestão da comunicação e transparência, exigindo em muitas situações a presença de especialistas, um considerável tempo e muita burocracia envolvidos.

A seção a seguir apresentará um estudo de caso com a aplicação dessas melhorias na Metodologia PETIC, avaliando se o resultado obtido é o esperado.

## 5 ESTUDO DE CASO

---

Esta seção apresenta o estudo de caso realizado para avaliar a eficiência das propostas de incorporar a gestão dos riscos e da comunicação na Metodologia PETIC. Por conveniência foi escolhida uma empresa sergipana atuante no segmento têxtil, com administração familiar e PE já consolidado. Em 2015 o PE de TIC passou a ser realizado com a utilização da Metodologia PETIC.

Neste capítulo, serão mostradas as etapas e diretrizes gerais para o estudo de caso, além do estudo desenvolvido na referida empresa.

### 5.1 ETAPAS E DIRETRIZES PARA O ESTUDO DE CASO

As principais etapas para a realização do estudo de caso foram as seguintes:

- Projeto do estudo de caso – definição dos objetivos e planejamento do estudo de caso;
- Preparação para a coleta de dados – definição dos procedimentos e protocolos para a coleta de dados;
- Coleta de evidências – execução e coleta de dados do estudo;
- Análise dos dados coletados;
- Consolidação e divulgação de resultados.

O detalhamento de cada uma dessas etapas será realizado nas próximas seções.

#### 5.1.1. PROJETO DO ESTUDO DE CASO

O objetivo principal do estudo de caso realizado é avaliar a suposição: *“A inclusão da gestão de riscos e de comunicação e transparência na Metodologia PETIC permitem a elaboração de um PE de TIC mais alinhado com os objetivos do negócio”*.

A Metodologia PETIC, com as propostas de melhorias sugeridas, foi aplicada na área de TIC de uma empresa sergipana do segmento têxtil, com histórico de PE e em fase de consolidação da implantação do PE de TIC formal.

O projeto iniciou em outubro de 2016 e finalizou fevereiro de 2017, tendo a participação do gerente de TIC (GTI), do coordenador de infraestrutura (CI), do analista de sistemas (AS), do gerente de qualidade (GQ) e do consultor de PE (CPE) da organização. Reuniões presenciais

periódicas foram realizadas, bem como comunicação por *e-mail* e aplicativos de videoconferência (*skype* e *appear.in*).

### 5.1.2. PREPARAÇÃO PARA A COLETA DE DADOS

Para atingir o objetivo definido do estudo de caso foi estabelecido o protocolo de estudo e alguns instrumentos de medição, apresentados no Quadro 8.

Quadro 8 - Indicadores de medição do estudo de caso

Grupo	Indicador
Catálogo de riscos de TIC	Número de riscos
	Número de riscos por categoria
	Número de riscos com ações de redução e contingência
	Número de riscos da organização
	Número de riscos da organização por categoria
	Número de riscos da organização com ações de redução e contingência
Catálogo de comunicação e transparência de TIC	Número de processos de comunicação e transparência
	Número de processos de comunicação e transparência da organização

Fonte: Autor (2017).

Os indicadores definidos e coletados para o estudo de caso são de fácil mensuração, sendo calculados por meio simples somatório.

Os resultados obtidos com os indicadores foram complementados com a aplicação de um questionário junto aos participantes do estudo de caso visando à realização de uma avaliação qualitativa do modelo proposto.

O questionário, chamado de Avaliação da Proposta de Melhorias da Metodologia PETIC, investigou as seguintes variáveis: eficácia, produtividade, segurança, satisfação, adequação, operacionalidade, acurácia e inteligibilidade. Além disso, reservou espaço para comentários.

### 5.1.3. COLETA DE EVIDÊNCIAS

A coleta de evidências refere-se à execução do estudo de caso, incluindo a coleta de dados, onde se verifica se os dados estão de acordo com o que foi definido e se são suficientes para a análise.

A seguir serão descritas as principais atividades realizadas no estudo de caso.

### 5.1.3.1. ESTUDO DE CASO COMPANHIA TÊXTIL

Em 2015 foi iniciado o projeto de utilização da Metodologia PETIC na organização visando estruturar formalmente as diretrizes, metas e objetivos da área de TIC em consonância com os objetivos e metas organizacionais. Este trabalho pioneiro permitiu uma maior visibilidade dos processos, necessidades e dificuldades da área, possibilitando um planejamento mais próximo da realidade.

Durante os preparativos para o PE da organização em 2016 foi apresentado o projeto para realização do estudo de caso da aplicação da Metodologia PETIC com as propostas de melhorias que se deseja incorporar ao seu escopo. Observou-se que, dentre as metas, a gestão de riscos e o desenvolvimento da comunicação se faziam presentes nas diretrizes estratégicas a serem discutidas para o ano de 2017.

Por conta disso o assunto foi bem aceito e a apresentação do projeto serviu até mesmo para suscitar questões sobre o tema e dirimir algumas dúvidas existentes. Como colocado verbalmente por alguns participantes, o risco normalmente é conhecido por todos e os envolvidos já sabem o que fazer quando ocorrer. No entanto, foi considerada necessária existência do registro formal dos possíveis riscos que podem ocorrer.

No âmbito da comunicação destacou-se no uso excessivo de *e-mail* e sem critério de destinatários, envolvendo muitos sem a devida necessidade.

Para a realização das atividades, foram utilizadas as seguintes ferramentas e técnicas: análise da matriz *SWOT*, *benchmarking*, opinião especializada, gráficos de tomada de decisão e gráficos de *Gantt*.

Para montagem do artefato PETIC o modelo proposto do *workflow* foi seguindo. A definição da missão e visão foi apenas atualizada diante da proposta da empresa que é a manutenção de no máximo cinco indicadores para cada uma das áreas envolvidas. No caso, por definição foram mantidos os quatro indicadores para área de TIC, a saber:

- Percentual de realização/atendimento dos chamados;
- Percentual de atendimento dos projetos;
- Tempo médio de atendimento;
- Disponibilidade dos ativos de TIC.

Não houve qualquer alteração no Catálogo de Processos da TIC, pois o mesmo já tinha sido montado e revisado no ano anterior. No entanto, já se sabe que para o PE de TIC de 2017 mudanças ocorrerão diante dos objetivos futuros da organização.



A continuidade da utilização da PETIC, com um nível de conhecimento maior da Metodologia, proporcionou avanços no planejamento, fato esse que pode ser observado na Tabela 17, pelo número de processos utilizados neste ano.

Tabela 17 - Utilização de processos do catálogo de processos de TIC

Indicador	Quantidade
Processos disponíveis no Catálogo de Processos de TIC	119
Processos utilizados do Catálogo de Processos de TIC - PE de TIC (2015)	68
Processos utilizados do Catálogo de Processos de TIC - PE de TIC (2016)	81

Fonte: Autor (2017).

A Tabela 18 abaixo identifica os processos de TIC, com suas respectivas áreas, que foram incorporados ao Catálogo de Processo da organização. Percebe-se que cerca de 54% dos processos são da área de Governança de TIC o que sinaliza uma preocupação da organização na implantação de ações voltadas à gestão e ao alinhamento com o negócio.

Tabela 18 - Relação de novos processos de TIC utilizados

Processo	Área
1.1.3 - Unificação do banco de dados	1 - Dados e informações
2.4.9 - Medição e análise	2 - <i>Software</i>
3.1.1 - Política de aquisição de equipamentos	3 - <i>Hardware</i>
3.2.3 - Redundância de <i>hardware</i>	3 - <i>Hardware</i>
3.3.1 - Processo de recuperação de desastres	3 - <i>Hardware</i>
4.1.4 - Serviço de VoIP	4 - Telecomunicações
3.3.1 - Processo de recuperação de desastres	6 - Governança de TIC
6.2.6 - Gerenciamento de nível de serviço	6 - Governança de TIC
6.2.7 - Gerenciamento de capacidade	6 - Governança de TIC
6.2.8 - Gerenciamento de disponibilidade	6 - Governança de TIC
6.2.9 - Gerenciamento de continuidade de serviços	6 - Governança de TIC
6.2.11 - Gerenciamento de fornecedor	6 - Governança de TIC
6.4.4 - Fornecimento da Governança de TIC	6 - Governança de TIC

Fonte: Autor (2017).

O processo Serviço de VoIP passou a ser considerado devido a instalação de novas centrais telefônicas nas unidades, as quais permitiram a implantação desse processo. Vale ressaltar que não havia planejamento ou previsão orçamentária para a aquisição, tendo ocorrido após a deliberação da alta direção da empresa.

No caso do processo Unificação do banco de dados, o mesmo se deu por conta da reestruturação dos servidores e por questões de licenciamento de *software*. Houve uma falha no PE de TIC de 2015, pois durante a sua elaboração a equipe não o selecionou, o que foi

devidamente corrigido nesta aplicação, expandindo sua abrangência para todos os setores estratégicos.

Os demais processos foram incluídos em função do avanço e aprendizado na utilização da Metodologia PETIC.

Para análise de maturidade dos processos optou-se por continuar e revisar a análise proposta pela PETIC. A revisão identificou que cinco processos tiveram o nível de maturidade elevado em relação ao ano anterior, migrando Nível 1 (mínimo) para o Nível 3 (satisfatório). Essa evolução se deu principalmente pela aplicação da PETIC no ano anterior e disponibilidade de uma visão mais clara e objetiva dos processos de TIC da empresa, permitindo a realização do planejamento das atividades, exceto o processo Serviço de telefonia fixa que recebeu investimentos financeiros não planejados. Segue abaixo a relação dos processos com mudança no nível de maturidade. Vale ressaltar que nenhum processo teve o nível de maturidade reduzido.

- Processo 1.1.4 – Disponibilidade do servidor;
- Processo 1.2.2 – Política de *backup*;
- Processo 2.2.4 – Desenvolvimento de *software*;
- Processo 3.2.4 – Monitoração da utilização de *hardware*;
- Processo 4.1.3 – Serviço de telefonia fixa.

O passo seguinte à definição do catálogo de processos de TIC da organização foi a priorização de cada um deles mediante a análise e critérios definidos pela PETIC, os quais foram mantidos, inclusive com a pontuação/peso e cálculo da importância. A alteração que ocorreu se concentrou no critério risco, que passou a utilizar o resultado da definição do catálogo da organização.

Até então, a Metodologia PETIC apenas pontuava o processo em relação ao risco e a proposta aqui apresentada passou a considerar, descrever e detalhar todos os riscos de TIC envolvidos com cada um dos processos. Neste cenário, pode-se avaliar com maior riqueza de detalhes os processos de TIC e seus riscos associados. A execução da etapa de definição do catálogo e do plano de resposta aos riscos de TIC foi executada com a participação do Gerente de TIC, do Coordenador de Infraestrutura e do Analista de Sistemas. Além das reuniões normais para elaboração do PE de TIC, as quais também o tema gestão de riscos foi discutido, foram realizadas outras quatro especificamente para tratar do assunto.

Na primeira reunião foram discutidas as estratégias para análise de definição do catálogo de risco de TIC da organização. O catálogo de riscos proposto (Apêndice A) foi apresentado para que cada uma avaliasse os riscos existentes e pudesse contribuir, seja descartando riscos ali

existentes que não fizessem parte do escopo da organização e/ou incluindo outros que não estavam descritos. A segunda reunião teve como pauta a análise e discussões do que cada um avaliou sobre o catálogo proposto e a realização das análises qualitativas e quantitativas, identificando assim os riscos prioritários e o tratamento a ser executado. A terceira e a quarta reuniões trataram da consolidação do plano de respostas aos riscos e as medidas a serem executadas.

O resultado final indicou a eliminação de três riscos que não se aplicavam à realidade da organização e, ao catálogo da organização foram adicionados outros dez, que referem a riscos específicos da empresa, seu contexto e realidade. Todos esses riscos denotaram ações de redução e contingência e servirão de base para avaliação do próximo PE de TIC.

A consolidação do Catálogo de Comunicação e Transparência de TIC se deu de modo mais rápido, em apenas uma das reuniões o catálogo proposto (Apêndice C) foi analisado e validado, com a exclusão de cinco itens de comunicação e adição de outros dois específicos da organização.

Após o cumprimento das atividades, uma nova versão do artefato PETIC foi concluída e submetida para avaliação, inclusive com a apresentação aos demais gestores da empresa. O projeto foi validado e finalizado.

#### **5.1.4. FORMA DE COLETA DAS EVIDÊNCIAS**

Para a coleta de dados e evidência foram utilizados os seguintes recursos: entrevistas, observação e aplicação de questionários que, em conjunto com os indicadores, possibilitaram avaliar a suposição.

#### **5.1.5. ANÁLISE DOS DADOS COLETADOS**

Para as análises qualitativas e quantitativas do estudo de caso foram analisados os resultados de todas as entrevistas, observações e os questionários respondidos. Além disso, os indicadores foram analisados para avaliar a suposição.

Como pode ser observado na Tabela 19, foram utilizados os seguintes indicadores para avaliação do Catálogo dos Riscos de TIC e sua aplicação: número de riscos, número de riscos com ações de redução e contingência, número de riscos da organização, número de riscos da organização por Categoria, número de riscos da organização com ações de redução e contingência.

Tabela 19 - Indicadores de avaliação - catálogo dos riscos de TIC

Indicador	Catálogo Proposto dos Riscos de TIC	Catálogo dos Riscos de TIC da organização
Número de riscos	76	83
Número de riscos – dados	10	13
Número de riscos – <i>software</i>	16	16
Número de riscos – <i>hardware</i>	8	10
Número de riscos – telecomunicações	11	13
Número de riscos – pessoas	9	12
Número de riscos – Governança de TIC	22	19

Fonte: Autor (2017).

O Quadro 9 apresenta a relação dos riscos de TIC que foram incluídos e excluídos do catálogo durante a etapa de definição do catálogo de riscos. Os itens que foram desprezados/excluídos foram motivados por, no momento atual, ter a mínima chance de ocorrer, como analisado pelos participantes. Os itens incluídos tiveram por motivação ocorrências reais de problemas que causaram ou que podem causar transtornos à organização.

Quadro 9 - Análise do catálogo de riscos

Riscos de TIC	Categoria	Status
Não existência de <i>site backup</i>	Dados	Incluído
Falha no <i>backup</i> /restauração do Banco de Dados	Dados	Incluído
Falha <i>robot</i> de <i>backup</i> (MSL2024)	Dados	Incluído
Vulnerabilidade pelo uso de dispositivos pessoais na rede corporativa	Hardware	Incluído
Furtos de ativos	Hardware	Incluído
Indisponibilidade da VPN	Telecomunicações	Incluído
Indisponibilidade do serviço de <i>e-Mail</i> nas nuvens	Telecomunicações	Incluído
Mudança de local de trabalho (cidade) da equipe de desenvolvimento de <i>software</i>	Pessoas	Incluído
Corte de pessoal	Pessoas	Incluído
Terceirização do serviço de desenvolvimento de <i>software</i>	Pessoas	Incluído
<del>Inadequada estrutura física da empresa</del>	<del>Governança de TIC</del>	<u>Excluído</u>
<del>Dificuldade na alocação ou contratação de terceiros</del>	<del>Governança de TIC</del>	<u>Excluído</u>
<del>Falta de apoio da alta direção</del>	<del>Governança de TIC</del>	<u>Excluído</u>

Fonte: Autor (2017).

Do total de riscos existentes no Catálogo de Riscos de TIC da organização, 25 não tinham qualquer tipo de tratamento, mesmo que de modo informal. No caso de 6 riscos havia consciência

da possibilidade de ocorrência do risco e com procedimento de contingência não registrado. Em outros 3, havia um registro formal com diretrizes para contingência em caso de ocorrência.

No que se refere à comunicação e transparência de TIC, os processos de Comunicação e Transparência do Catálogo Proposto totalizam 15 itens de informação. Durante a análise e execução do PETIC, 5 itens foram desconsiderados por não terem relação com a empresa estudada e outros dois incluídos, como observado no Quadro 10.

Quadro 10 – Análise do catálogo de comunicação e transparência de TIC

Item	Descrição	Status
8.1	Resultados periódicos dos indicadores de TIC	Mantido
8.2	Interrupção ou indisponibilidade dos Serviços de TIC	Mantido
<del>8.3</del>	<del>Catálogo de Produtos e Serviços de TIC</del>	<del>Excluído</del>
<del>8.4</del>	<del>Divulgação dos Projetos de TIC</del>	<del>Excluído</del>
8.5	Divulgação missão, visão, objetivos e metas de TIC	Mantido
8.6	Comunicação sobre ocorrência dos riscos catalogados	Mantido
8.7	Orientação quanto ao uso dos recursos de TIC	Mantido
<del>8.8</del>	<del>Política de Segurança da Informação</del>	<del>Excluído</del>
8.9	Notificação do uso indevido dos recursos de TIC	Mantido
8.10	Notificação das alterações e manutenções nos <i>softwares</i> , sistemas ou ERP	Mantido
<del>8.11</del>	<del>Informação sobre a aplicação dos recursos financeiros na área de TIC</del>	<del>Excluído</del>
8.12	Notificação sobre contratações e desligamentos de componentes da equipe de TIC	Mantido
8.13	Comunicação de alterações em prazos e prioridades acordados com os usuários	Mantido
8.14	Papéis e responsabilidades do pessoal de TIC	Mantido
<del>8.15</del>	<del>Escala de trabalho da equipe de TIC</del>	<del>Excluído</del>
8.16	Boletim de Segurança da Informação	Incluído
8.17	Sensibilização quanto ao uso da TIC	Incluído

Fonte: Autor (2017).

Os itens 8.3 e 8.4 foram descartados por questões estratégicas do setor de TIC. No caso do item 8.8 por estar em processo de revisão e implantação, mas constará no catálogo de comunicação e transparência de TIC do PE de TIC de 2017, visto que deverá ser formalmente implantada no segundo semestre. Em relação ao item 8.11, a área de Orçamento já apresenta os valores, não só da TIC como das demais áreas. Já o item 8.15 foi descartado devido ao tamanho reduzido da equipe e não realização de trabalhos em regime de plantão ou sobreaviso.

A inclusão do item 8.16 deve-se ao fato de preparar, orientar e educar os colaboradores no que se refere a itens de segurança da informação sejam eles no ambiente do trabalho ou até mesmo pessoal, tendo em vista incidentes que ocorreram internamente que provocaram algum tipo de transtorno operacional. A ideia é disponibilizar periodicamente dicas para garantia da segurança. O item 8.17 trata de educar e sensibilizar o pessoal quanto ao devido uso e

conservação dos recursos de TIC na organização, por meio de palestras e *workshops* durante as reuniões operacionais existentes.

Como consequência a aplicação da Metodologia PETIC e a proposta de melhorias, a proposta de orçamento para área de TIC aumentou significativamente em relação aos anos anteriores. Percebeu-se que as demandas para esses investimentos sempre existiram, porém não estavam visíveis e declaradas. A partir do momento em que foram destacadas e associadas com os respectivos processos e, até mesmo riscos, foi possível realizar um orçamento mais preciso e o PE de TIC possibilitou a explicação com mais facilidade.

Pode ser observado no Quadro 11, o resultado da avaliação qualitativa da aplicação da metodologia de acordo com cada um dos itens e de acordo com possibilidades de resposta que compreendiam *Péssimo*, *Ruim*, *Regular*, *Bom* e *Excelente* as quais foram atribuídas pesos de 1 a 5 respectivamente, permitindo assim uma quantificação média das avaliações.

Quadro 11 - Resultado da avaliação qualitativa das propostas de melhorias na Metodologia PETIC

Item	Descrição	GTI	CI	AS	GQ	CPE	Média
Eficácia	Capacidade em atingir as metas especificadas	Ótimo	Ótimo	Ótimo	Ótimo	Ótimo	Ótimo
Produtividade	Emprego adequado dos recursos em relação à eficácia	Bom	Ótimo	Regular	Regular	Ótimo	Bom
Segurança	Nível aceitável de riscos em relação a aplicação	Ótimo	Ótimo	Regular	Regular	Ótimo	Bom
Satisfação	Capacidade de satisfazer os usuários em relação aos objetivos	Ótimo	Ótimo	Ótimo	Ótimo	Ótimo	Ótimo
Adequação	Capacidade em prover funções adequadas ao atingimento dos objetivos	Ótimo	Ótimo	Ótimo	Ótimo	Ótimo	Ótimo
Operacionalidade	Capacidade em permitir a operação e controle	Bom	Ótimo	Regular	Regular	Ótimo	Bom
Acurácia	Capacidade de prover, com precisão, resultados esperados	Ótimo	Ótimo	Ótimo	Ótimo	Ótimo	Ótimo
Inteligibilidade	Capacidade de possibilitar a compreensão da apropriação da proposta e como ela pode ser usada	Ótimo	Ótimo	Ótimo	Ótimo	Ótimo	Ótimo
Opções de Resposta: [1] - Péssimo [2] - Ruim [3] - Regular [4] - Bom [5] – Ótimo							

Fonte: Autor (2017).

Nota-se que dois participantes classificaram três itens com uma avaliação *Regular*, sendo eles Produtividade, Segurança e Operacionalidade. Por meio de entrevistas, comentários no questionário e observação identificou-se que a classificação dada foi em função única e exclusivamente da utilização de Planilha Eletrônica em vez de um *software*.

## 5.2 CONSIDERAÇÕES FINAIS DO CAPÍTULO

Este capítulo apresentou as etapas e diretrizes para a realização do estudo de caso. Tratou inicialmente sobre o projeto do estudo de caso e seu objetivo principal em avaliar a suposição da pesquisa se “*a inclusão da gestão de riscos e de comunicação e transparência na Metodologia PETIC permitem a elaboração de um PE de TIC mais alinhado com os objetivos do negócio*”.

Os resultados sinalizam que a suposição apresentada foi evidenciada, principalmente com a análise mais aprofundada dos processos de TIC e dos riscos associados a cada um deles. Ao final do trabalho, a área de TIC passou a dispor de um documento, mais precisamente o Artefato PETIC, apresentando um diagnóstico dos processos da área, o que permite alinhar suas metas e objetivos com os do negócio, concentrando forças e investimentos no que contribui e agrega valor para a TIC e para a organização.

O grande desafio que surge, a partir de agora, é monitorar, controlar e manter a gestão dos processos, dos riscos de TIC e da comunicação e transparência de modo a operacionalizar tudo o que foi identificado.

Há de se considerar, na análise deste estudo de caso, o fato de que a escolha da empresa se deu por conveniência pelo fato do autor ocupar o cargo de Gerente de TIC. Se por um lado representa uma facilidade devido ao apoio na execução das tarefas, não só pelo interesse acadêmico, como também profissional, por outro pode em algum momento proporcionar a condução dos trabalhos de modo imparcial. Apesar disso, os resultados foram satisfatórios em ambos os aspectos.

Outro ponto importante a ser ressaltado é que a suposição foi evidenciada na empresa estudada, mas é necessário aplicar a metodologia em outras organizações e com outras situações diferentes para que assim sejam proporcionadas outras melhorias à Metodologia PETIC.

## 6 CONSIDERAÇÕES FINAIS

---

Esta dissertação descreveu a preparação e aplicação do *survey* sobre as práticas de Governança de TIC utilizadas pelas empresas sergipanas para o alinhamento estratégico entre TIC e negócio. Também foram apresentadas as propostas de melhorias na Metodologia PETIC. Por meio da revisão da literatura foi mostrada a importância, para as organizações, do PE, do PE de TIC, do alinhamento estratégico entre TIC e negócio, da utilização de práticas de Governança de TIC e uma breve descrição sobre a Metodologia PETIC, desenvolvida pelo DCCOMP da Universidade Federal de Sergipe.

Na aplicação do *survey*, cujo público-alvo foram os CIOs das empresas sergipanas, identificou-se o panorama de adoção de práticas de Governança de TIC nas empresas do estado. As práticas de Governança de TIC mais utilizadas foram identificadas e listadas, bem como as principais vantagens e dificuldades apontadas pelos gestores para implantação e uso do alinhamento estratégico entre o PE da organização e o PE de TIC.

Atestou-se também que as empresas sergipanas utilizam pelo menos uma prática de Governança de TIC na definição do PE de TIC e para obter o alinhamento estratégico com o negócio. Também foi verificado que não há um consenso quanto ao conhecimento da alta direção das empresas acerca da necessidade e importância do alinhamento estratégico da TIC com o negócio.

Em especial foram apresentadas as propostas de melhorias da Metodologia PETIC. Objetivamente as propostas visaram incluir a gestão de riscos e da comunicação de transparência na elaboração do PE de TIC com o intuito de minimizar problemas relacionados ao gerenciamento dos riscos e das comunicações apontados pelos CIOs na análise do *survey*. Por consequência, também foi necessário alterações no *workflow* da Metodologia PETIC para comportar as propostas citadas.

Essencialmente, as propostas procuraram alinhamento com os conceitos estabelecidos pelos principais *frameworks* e modelos de Governança de TIC existentes na literatura e apontados no *survey*.

Foi percorrido sobre o estudo de caso realizado em uma empresa sergipana aplicando a Metodologia PETIC com as melhorias propostas. Nesta etapa, foram utilizadas algumas técnicas para confirmação da suposição, por meio da observação, questionários, entrevistas e indicadores. Por fim, foi realizada uma análise acerca dos resultados obtidos.



Como resultado da análise indicada no presente trabalho, inferiu-se que a Metodologia PETIC foi aprimorada. É sabido que a coleta de dados foi prejudicada em razão dos estudos não terem sido executados em sua plenitude, não permitindo avaliar todos os aspectos da Metodologia PETIC. No entanto, os dados coletados e os resultados obtidos denotam fortes indícios sobre a aplicabilidade das propostas.

A análise permitiu inferir que por meio das propostas de melhorias da Metodologia PETIC, é possível aprimorar o PE de TIC, proporcionando um melhor alinhamento com as estratégias do negócio e visando a garantia da continuidade dos serviços de TIC. Isso foi realizado pela incorporação de instrumentos para a gestão de riscos e da comunicação e transparência, atendendo perfeitamente as necessidades da organização alvo do estudo de caso, disponibilizando recursos para apoio na tomada de decisões e no planejamento das ações de TIC. Evidencia-se, assim, a suposição apresentada.

No entanto, cabe ressaltar que os resultados não são conclusivos quando aplicados em outro contexto ou em outras organizações. Ou seja, mesmo que a suposição tenha sido evidenciada para o estudo de caso realizado, não se pode extrapolar o mesmo resultado das propostas apresentadas em outras organizações, cabendo assim uma nova pesquisa com a aplicação em outras empresas.

## **6.1 PRINCIPAIS CONTRIBUIÇÕES**

A execução deste trabalho proporcionou várias contribuições, sejam no âmbito da academia, da indústria e pessoal.

Em se tratando da academia e da indústria, pode-se citar inicialmente a aplicação de técnicas de pesquisa em temas que interessam diretamente a indústria, como planejamento e alinhamento estratégico, Governança de TIC, gestão de riscos e da comunicação e transparência permitindo uma comparação da teoria com a prática, resultando em propostas teóricas que podem ser aplicadas diretamente na indústria.

Outra contribuição importante está relacionada com a manutenção do aperfeiçoamento constante da Metodologia PETIC oriunda do meio acadêmico local e utilizada em diversas organizações, e atendendo as necessidades delas, proporcionando uma maior efetividade e com simplicidade na execução do PE de TIC.

O estudo se revelou pioneiro no estado, apresentando um quadro de características de utilização das práticas de governança de TIC no estado de Sergipe, tornando-se fonte de referência para outras pesquisas.

Em termos pessoais, este trabalho representou aumento de conhecimento em técnicas de pesquisa, em temas relacionados com a TIC, tais como gestão e governança, bem como se torna uma ponte para a obtenção de um título acadêmico que possibilitará atingir outros objetivos.

## 6.2 CONSOLIDAÇÃO E DIVULGAÇÃO DOS RESULTADOS

Os resultados foram consolidados na presente dissertação e em alguns artigos que estão sendo submetidos em conferências e periódicos nacionais e internacionais. Significativa parcela dos resultados já foi publicada em duas conferências de âmbito internacional:

- Governança de TIC: um panorama da adoção das práticas em empresas do estado de Sergipe, Brasil – CibSE2016 (B4) – Artigo submetido e aceito, porém por falta de recursos financeiros não foi possível apresentá-lo;
- *ICT Governance, Risks and Compliance: a systematic quasi-review* – ICEIS-2017(B1);
- A adoção de práticas de governança de TIC na gestão dos processos de negócio e de *software*: um *survey* no âmbito das empresas sergipanas – Artigo em desenvolvimento.

## 6.3 LIMITAÇÕES E DIFICULDADES DA PESQUISA

No que se refere às limitações e dificuldades da pesquisa, podem ser citadas:

- Limitação de tempo devido à necessidade de várias atividades até a execução do estudo de caso, tais como: revisão da literatura; preparação, planejamento, aplicação e análise do *survey*; análise das práticas de governança; definição dos componentes e preparação e aplicação do estudo de caso;
- A resistência da comunidade em participar de pesquisas, sendo necessário um esforço extra, mantendo contato com participantes potenciais, para que os mesmos respondessem o *survey*;
- A dificuldade das empresas em aplicar novos modelos e metodologias em seu ambiente, normalmente relacionada com restrições financeiras, de tempo e de recursos humanos, ou até mesmo por não permitirem a presença de terceiros em suas dependências;
- A indisponibilidade do *software* de apoio PETIC para a elaboração do PE de TIC resultou na utilização de planilhas eletrônicas, elevando o tempo e o esforço de trabalho.

## 6.4 TRABALHOS FUTUROS

As análises realizadas sobre a aplicação do *survey* sobre as práticas de governança de TIC utilizadas pelas empresas sergipanas para o alinhamento estratégico entre TIC e negócio e a avaliação do estudo de caso suscitou a possibilidade de trabalhos futuros com o intuito de investigar alguns aspectos importantes, mas que por limitação de tempo ou por, inicialmente não terem sido objetos de estudo não constaram no presente trabalho.

Inicialmente se propõe a avaliar a aplicação das propostas de melhorias em outras organizações, de diferentes segmentos, ramos de atuação e tamanho, possibilitando assim uma análise mais apurada de eficiência das propostas. Quanto maior a aplicação prática, maiores as possibilidades de sucessos e aperfeiçoamento da metodologia.

Consequentemente sugere-se a informatização das propostas, otimizando o tempo de aplicação, segurança no registro e armazenamento dos dados e análise das informações.

No âmbito da realização do PE, cabe pesquisar dentro das organizações o percentual de realização do PE de TIC diante do que é proposto, ou seja, ao longo do ano e diante das metas e objetivos propostos, quanto foi realizado. Esta questão revela-se importante, pois é possível que em muitas organizações exista o PE e o PE de TIC formais, porém os mesmos não são efetivamente realizados. Diante disso, investigar os fatores de sucesso e insucesso na execução do PE e do PE de TIC.

## REFERÊNCIAS

---

- AAKER, D. A.; KUMAR, V.; DAY, G. S. Pesquisa de Marketing. 1ª ed. São Paulo: Atlas. 2004.
- ATESE, M.; TANRIÖVER, Ö. Investigation of the Cobit Framework's Input\Output Relations by Using Graph Metrics. Federated Conference on Computer Science and Information Systems, 2014. Proceedings 2014, pp. 1269–1275.
- AUDY, J. L.; BRODBECK, A. F. Sistemas de informação: planejamento e alinhamento estratégico nas organizações. São Paulo: Atlas, 2003.
- AZEVEDO, E. F. Y. O papel estratégico da Tecnologia da Informação na área da saúde. Dissertação. PUC-CAMPINAS, 2013.
- BABBIE, E. Métodos de Pesquisas de Survey Tradução Guilherme Cezarino. Belo Horizonte: Ed. UFMG, 519 p. 1999.
- BASIL, V.; WEISS, D. A Methodology for Collecting Valid Software Engineering Data. In: IEEE Transactions on Software Engineering. Vol 10(3): 728-738. 1984
- BERMEJOA, P. H. S.; TOBELLIB, A. O.; ZAMLADEA, A. L.; SANTOS, P. A.; ZYPPO, L. Evaluating IT Governance practices and business and IT outcomes: A quantitative exploratory study in Brazilian companies. In CENTERIS 2014 –Conferenceon Enterprise Information Systems / Projman 2014 – International Conferenceon Project Management / HCIST 2014 –International Conferenceon Health and Social Care Information Systems and Technologies, Volume 16, 2014. pp. 849-857.
- BRODBECK, A. F. Alinhamento estratégico entre os planos de negócio e de tecnologia de informação: um modelo operacional para a implementação. Dissertação. UFRGS. 2001.
- BRODBECK, A. E HOPPEN, N. – Alinhamento Estratégico entre Planos de Negócio e de Tecnologia de Informação: um Modelo Operacional para Implementação. Revista de Administração Contemporânea. v.7, n.3, p.9-33, Jul./Set. 2003.
- CARISSIMI, Leonardo. Gestão de Riscos e os Cisnes Negros do mundo digital. Disponível em:[http://convergecom.com.br/tiinside/seguranca/artigos-seguranca/11/03/2016/gestao-de-riscos-e-os-cisnes-negros-do-mundo-digital/?noticiario=SG\\_](http://convergecom.com.br/tiinside/seguranca/artigos-seguranca/11/03/2016/gestao-de-riscos-e-os-cisnes-negros-do-mundo-digital/?noticiario=SG_). Acesso em: 01, abr, 2017.
- CHAN, Y. E.; HUFF, S. L.; BARCLAY, D.; COPELAND, D. G. Business Strategic Orientation, Information Systems Strategic Orientation, and Strategic Alignment. Information Systems Research, v.8, n.2, p-125- 150, Jun. 1997.
- CHIAVENATO, I.; ARÃO, S. Planejamento Estratégico – Fundamentos e Aplicações, Rio de Janeiro: Elsevier Editora Ltda. 2004.
- CMMI INSTITUTE (CMMI). A framework for improving performance. Disponível em: <<http://cmmiinstitute.com/>>. Acesso em: 19 Jul 2015.
- CONFEDERAÇÃO NACIONAL DAS INDÚSTRIAS (CNI). . Perfil da Indústria nos Estados. Disponível em <<http://perfilestados.portaldaindustria.com.br/estado/se>>, Acesso em 08, oct, 2016.
- DRUCKER, P. Introdução a Administração, São Paulo, Pioneira, 1984.

FACHIN, O. Fundamentos de metodologia. São Paulo: saraiva. 2001.

FONSECA, J. J. S. Metodologia da pesquisa científica. Fortaleza: UEC, 2002. Apostila.

GARTNER Inc. Use Six Principles of Resilience to Address Digital Business Risk and Security. Disponível em: <https://www.gartner.com/doc/3104129?ref=clientFriendlyURL>. Acesso em 01, abr, 2017.

GERHARDT, T. E.; SILVEIRA, D. T. (Org.). Métodos de pesquisa. Porto Alegre: Ed. da UFRGS, 2009. (Educação a Distância, 5). Disponível em: [http://www.lti.pro.br/userfiles/downloads/13\\_Livro\\_Metodos\\_de\\_Pesquisa.pdf](http://www.lti.pro.br/userfiles/downloads/13_Livro_Metodos_de_Pesquisa.pdf). Acesso em 17, dez, 2016.

GIL, A. C. Métodos e Técnicas de Pesquisa Social. 5ª ed. São Paulo: Atlas, 1999.

HENDERSON, J.; VENKATRAMAN, N. Strategic Alignment: Leveraging Information Technology for Transforming Organizations. IBM Systems Journal, v.32, n.1, 1993.

HIRSCHHEIM, R.; SABHERWAL, R. Detours in the path toward strategic information systems alignment. California Management Review, v.44, n.1, p.87-108, 2001.

INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION (ISACA). WhatIsCobit5?:It's the leading framework for the Governance and management of enterprise IT. Disponível em: <http://www.isaca.org/COBIT/Pages/default.aspx>. Acesso em: 19 Jul. 2015.

ITIL. What is ITIL. Disponível em: <https://www.axelos.com/best-practice-solutions/itil/what-is-itil>. Acesso em: 19 Jul. 2015.

JAANA, M.; TEITELBAUM, M.; ROFFEY, T. IT Strategic Planning in a Pediatric Hospital: Overview of the Process and Outcomes. HICSS 2012. Proceedings, 2012, pp. 2910=2919.

KASPERSKY. Things to do before the next big thing: How the financial industry reacts to cyberthreats. Disponível em: <https://business.kaspersky.com/how-the-financial-industry-reacts-to-cyberthreats/6610/>. Acesso em 01, abr, 2017.

KATAEV, M.; BULYSHEVA, L. A System for Strategic and Tactical Planning of Industrial Enterprise Based on Business Processes. Enterprise Systems Conference (ES) 2014, pp. 33-35.

KILIÇ, N.; METIN, B. Importance of Education in Information Technology Governance. Proc. of 4th IEEE International Symposium on Logistics and Industrial Informatics, 2012. pp. 65-68.

KOTLER, P. Administração de Marketing: análise, planejamento, implementação e controle. 5 ed. São Paulo: Atlas, 1998.

LABADESSA, E. O SAP e a Governança de TI: suas contribuições para as melhores práticas nas organizações. Revista Metropolitana de Sustentabilidade-RMS, v. 1, n. 1, p. 44-55, 2011.

LAKATOS, E. V.; MARCONI, M. A. Metodologia Científica. 5ª ed. São Paulo: Atlas, 2007.

LAURINDO, F. J. Tecnologia da Informação: Planejamento e Gestão de Estratégias. São Paulo: Atlas, 2008, 400p.

LIMA, R. Planejamento estratégico alinhado com a tecnologia da informação. II Congresso de Pesquisa e Inovação da Rede Norte Nordeste de Educação Tecnológica. João Pessoa. 2007.

LIRA, L. M. B. Elaboração de um artefato de Planejamento Estratégico de TIC para o CPD/UFAM, baseado na Metodologia PETIC. Dissertação de Mestrado. UFAM, 2011.

- MAKHLOUF, M.; ALLAL-CHERIF, O. Pertinence and feasibility of a unifying holistic approach of IT governance. In: System Sciences (HICSS), 2015 48th Hawaii International Conferenceon. IEEE, 2015. p. 4575-4584.
- MARCHI, L. O. Guia de Uso para o PETIC 2.0. Relatório Técnico. DCOMP, UFS. São Cristóvão, 2010.
- MARCOS, A. F.; ROUYET, J. I.; BOSH, A. An IT Balance Scorecard Design under Service Management Philosophy. HICSS 2012.Proceedings, 2012, pp. 4972–4981.
- MARTINS, G. A. Manual para elaboração de monografias e dissertações. 3. ed. São Paulo: Atlas, 2002.
- MAY, T. Pesquisa Social - questões, métodos e processos. Trad. Carlos A. S. Netto Soares. Porto Alegre, RS: Artmed, 2004.
- NASCIMENTO, R. P. C. Metodologia PETIC - Planejamento Estratégico de TIC. Aracaju [s.n], 2011.
- OLIVEIRA, S. L. Tratado de metodologia científica. São Paulo: Pioneira. 1997.
- PALMEIRA, J. C. PETIC 3.0: Proposta de Aperfeiçoamento da Metodologia PETIC. Dissertação de Mestrado. Universidade Federal de Sergipe - Centro de Ciências Exatas e Tecnológicas. 2012.
- PALMEIRA, J. C.; NETO, D. A. C.; NASCIMENTO, R. P. C. PETIC Wizard proposal: A software tool for support PETIC methodology. In Proceedings of the 6th Euro American Conference on Telematics and Information Systems (pp. 407–411). New York, NY, USA: ACM., 2012.
- PARVISI, R.; OGHBAEI, F.; KHAYAMI, S.R. Using COBIT and ITIL frameworks to establish the alignment of business and IT organizations as one of the critical success factors in ERP implementation. In Information and Knowledge Technology (IKT), 2013 5th Conferenceon. 2013. IEEE. pp. 274-278.
- PEREIRA, R.; MIRA DA SILVA, M. Towards na Integrated IT Governance and IT Management Framework. Proc. 16th International Conferenceon Enterprise Distributed Object Computing (EDOC), IEEE Press, 2012a, pp. 191-200.
- PERSSE, J. Project Management Success with CMMI: 7 CMMI Process Areas. Pearson Education. 2007
- PINA, E. C.; PALMEIRA, J. Planejamento Estratégico de Tecnologia da Informação e Comunicação: Estudo de Caso CPD/UFS e TRE/SE. São Cristóvão, 2010.
- PINHEIRO, M. G.; MISAGHI, M. Proposal of a Framework of Lean Governance and Management of Enterprise IT. 14 Proceedings of the 16th International Conferenceon Information Integration and Web-based Applications & Services, 2014. pp. 554-558.
- PROJECT MANAGEMENT INSTITUTE (PMI). PMBOK® Guide and Standards. Disponível em: <<http://www.pmi.org/>>. Acesso em: 05 Out 2015.
- REICH, B. H.; BENBASAT, I. Measuring the Linkage between Business and Information Technology Objectives. MIS Quarterly, v.20, n.1, p.55-81, Mar. 1996.
- ROCHA, Fábio Gomes. Um modelo automatizado para apoio à tomada de decisão estratégica em TIC.62f. Dissertação (Mestrado) - Departamento de Ciência da Computação, Universidade Federal de Sergipe, 2017.
- ROGÉRIO, F. C. Planejamento Estratégico de Tecnologia da Informação Orientado ao Alinhamento de Negócio das Empresas: o Caso do Grupo de CIOS de Santa Catarina. Dissertação de Mestrado. Universidade do Estado de Santa Catarina - Centro de Ciências da Administração. 2007.

- REZENDE, D. A. Tecnologia da Informação e Planejamento Estratégico. Rio de Janeiro: Brasport, 2011.
- \_\_\_\_\_. Planejamento de Sistemas de Informação e Informática: Guia prático para planejar Tecnologia da Informação integrada ao Planejamento Estratégico das Organizações. 4ª ed. São Paulo: Atlas, 2011, 200p.
- SHIVASHANKARAPPA, A. N.; DARMALINGAM, R.; SMALOV, L.; ANBAZHAGAN, N. Implementing IT Governance Using Cobit: A Case Study Focusing on Critical Success Factors. World Congress on Internet Security. (WorldCIS-2012). IEEE, 2012. pp. 144-149. SHIVASHANKARAPPA et al., 2012)
- TAROUCO, H. H.; GRAEML, A. R. Governança de tecnologia da informação: um panorama da adoção de modelos de melhores práticas por empresas brasileiras usuárias. Revista de Administração, v. 46, n. 1, p. 07-18, 2011.
- TEO, T. S. H.; KING, W. R. Integration between business planning and information systems planning: na evolutionary-contingency perspective. Journal of Management Information Systems. V.14, n.1, p-185-214, 1997.
- TEXTOR, A.; GEIHS, K. Calculation of COBIT Metrics Using a Formal Ontology. IFIP/IEEE IM 2015 Workshop: 10th International Workshop on Business-driven IT Management (BDIM), 2015. pp 1384-1390.
- TRIBUNAL DE CONTAS DA UNIÃO (TCU). “Perfil de Governança de TI”. Disponível em: <<http://portal.tcu.gov.br/comunidades/fiscalizacao-de-tecnologia-da-informacao/atuacao/perfil-de-governanca-de-ti/>>. Acesso em: 26 Jul. 2015.
- TORRES, O. F. F. Curso de engenharia econômica e análise de riscos no CEGP. São Paulo: FCAV / POLI-USP, 2002.
- VAN, S. R.; BERGHOUT, E. The Goal/ Question /Metric Method: A practical guide for quality improvement of software development. McGraw-Hill. 1999.
- WEILL, P.; ROSS, J. W. IT-Governance: How top performers manage IT decision rights for superior results. USA: Havard Business Press, 2004.
- \_\_\_\_\_. Governança de Tecnologia da Informação. Editora M. Books, 2005.
- WRIGHT, P.; KROLL, M. J.; PARNELL, J. Administração estratégica: conceitos. São Paulo, Editora Atlas, 2009.
- VENKATRAMAN, N. Beyond outsourcing: managing IT resources as a value center. Sloan Management Review, v. 38, n. 3, p. 51-64, Spring 1997.
- VERGARA, S. C.. Projetos e relatórios de pesquisa em administração. São Paulo: Atlas, 2000.
- YIN, R. K. Estudo de caso – planejamento e métodos. 2ª Ed. Porto Alegre: Bookman. 2001.

**APENDICES**

---



## APENDICE A – CATÁLOGO DE RISCOS DE TIC

ID	Riscos de TIC	Categoria	Processo PETIC	Probabilidade	Impacto	Impacto Financeiro	VME	Prioridade	Tratamento
7.1	Falha na instalação, configuração ou administração do Banco de Dados.	Dados	1.1.1 - Administração do Banco de Dados.						
7.2	Indisponibilidade do servidor (arquivos, banco de dados)	Dados	1.1.4 – Disponibilidade do servidor.						
7.3	Falta de capacidade e/ou redundância para armazenamento dos dados	Dados	1.1.5 – Preparação para crescimento/escalabilidade 1.2.1 – Disposição de discos rígidos						
7.4	Política de backup inexistente ou inadequada	Dados	1.2.2 – Política de backup						
7.5	Indisponibilidade de mídias de <i>backup</i>	Dados	1.2.3 – Disposição de mídias de <i>backup</i>						
7.6	Acesso não autorizado às informações	Dados	1.3.2 – Controle de acesso						
7.7	Espionagem industrial	Dados	1.3.2 – Controle de acesso						
7.8	Vazamento ou perda de dados e informações	Dados	1.3.2 – Controle de acesso						
7.9	Perda de documentação e/ou código-fonte de <i>softwares</i>	Dados	1.2.2 – Política de backup						
7.10	Sabotagem no código-fonte	Dados							
7.11	Falta de equipe capacitada para desenvolvimento das atividades	<i>Software</i>	2.2.1 – Suporte a programas						
7.12	Instalação e uso de <i>softwares</i> não licenciados	<i>Software</i>	2.2.2 – Política de Licenciamento de <i>softwares</i>						
7.13	Indisponibilidade dos Sistemas, ERP, portais e <i>sites</i> .	<i>Software</i>	2.3 – <i>Softwares</i> de suporte para o negócio						
7.14	Falha na definição ou indefinição das necessidades e prioridade dos usuários (requisitos não definidos claramente)	<i>Software</i>	2.4.1 – Gerência de Requisitos						
7.15	Falha no desenvolvimento ou retrabalho devido a requisitos mal definidos	<i>Software</i>	2.4.3 – Solução Técnica						
7.16	Testes e homologações mal realizados	<i>Software</i>	2.4.5 – Verificação 2.4.6 – Validação 2.4.8 – Garantia da Qualidade de Processo e de Produto						
7.17	Falha na implantação	<i>Software</i>	2.4.7 – Gerência de Configuração						
7.18	Não aquisição de licenças associadas ao novo software	<i>Software</i>	2.2.3 - Política de Licenciamento de Software						
7.19	Falhas no processo de migração de dados	<i>Software</i>	2.3.1 - Software de suporte para o Negócio						
7.20	Não migração dos sistemas legados	<i>Software</i>	2.3.1 - Software de suporte para o Negócio						
7.21	Indisponibilidade de serviços bancários <i>on line</i> (versão do java)	<i>Software</i>	2.3.4 - Softwares aplicativo para escritório						
7.22	Aquisição de <i>software</i> inadequado ao processo do negócio	<i>Software</i>	2.4.13 - Adquirir e manter software aplicativo						
7.23	Falha de integração dos novos <i>softwares</i> com	<i>Software</i>	2.4.13 - Adquirir e manter software						

	sistemas legados		aplicativo						
7.24	Alterações nos processos, requisitos e regras de negócio durante o desenvolvimento do <i>software</i> .	<i>Software</i>	2.4.2 - Desenvolvimento de Requisitos						
7.25	<i>Software</i> desenvolvido não atende às exigências dos processos organizacionais	<i>Software</i>	2.4.5 – Verificação						
7.26	Falha no processo de testes e homologação do <i>software</i>	<i>Software</i>	2.4.6 – Validação						
7.27	Falta de manutenção de <i>hardware</i>	<i>Hardware</i>	3.2.1 – Manutenção preventiva 3.2.2 – Manutenção corretiva						
7.28	Falta de <i>hardware</i> de <i>backup</i> para serviços críticos	<i>Hardware</i>	3.2.3 – Redundância de <i>hardware</i>						
7.29	Não continuidade dos serviços de TIC após desastres (naturais, vandalismo, incêndios, etc)	<i>Hardware</i>	3.3.1 – Processo de recuperação de desastres						
7.30	Falta de energia	<i>Hardware</i>	3.3.2 – Proteção contra falhas de energia						
7.31	Falta de experiência da equipe de desenvolvimento TIC	<i>Hardware</i>	2.2.1 - Suporte a programas						
7.32	Atraso na entrega do <i>hardware</i>	<i>Hardware</i>	3.1.1 - Política de aquisição de equipamentos						
7.33	Dimensionamento inadequado do <i>hardware</i> para novo <i>software</i>	<i>Hardware</i>	3.1.3 - Dimensionamento da utilização do <i>hardware</i>						
7.34	Sobrecarga da rede e servidores	<i>Hardware</i>	3.1.3 - Dimensionamento da utilização do <i>hardware</i>						
7.35	Indisponibilidade da Central Telefônica	Telecomunicações	4.1.1 – Ramais telefônicos						
7.36	Indisponibilidade do Serviço de Telefonia Móvel	Telecomunicações	4.1.2 – Serviço de telefonia móvel						
7.37	Indisponibilidade do Serviço de Telefonia Fixa	Telecomunicações	4.1.3 – Serviço de telefonia fixa						
7.38	Uso indevido do <i>e-mail</i>	Telecomunicações	4.2.1 – Utilização de <i>e-mail</i>						
7.39	Acesso indevido ou não autorizado à rede, ativos e recursos de TIC.	Telecomunicações	4.3.1 – Controle de usuários 4.3.2 – Controle de acesso a arquivos e recursos						
7.40	Indisponibilidade da rede física	Telecomunicações	4.3.3 – Estrutura de rede física						
7.41	Indisponibilidade da rede sem fio	Telecomunicações	4.3.4 – Estrutura de rede sem fio						
7.42	Acesso ou uso indevido da <i>internet</i>	Telecomunicações	4.4.1 – Política de acesso à <i>internet</i> 4.4.2 – <i>Firewalls</i> 4.4.4 – Política de segurança						
7.43	Vulnerabilidade quanto a ataques externos ou <i>softwares</i> maliciosos	Telecomunicações	4.4.4 – Política de segurança						
7.44	Indisponibilidade do serviço ou <i>link</i> de <i>internet</i>	Telecomunicações	4.4.3 – Dimensionamento de banda 4.4.6 – Disponibilidade do servidor 4.4.7 – Controle de tráfego						
7.45	Vulnerabilidade do antivírus e/ou <i>firewall</i>	Telecomunicações	4.4.2 - <i>Firewalls</i>						
7.46	Contratação de pessoal não qualificado ou apto para desenvolvimento das funções	Pessoas	5.1.2 – Recrutamento e seleção						
7.47	Desmotivação da equipe de TIC e/ou perda de talentos	Pessoas	5.1.3 – Plano de carreira 5.1.5 – Remuneração 5.1.6 – Liderança e Gestão de Equipe						
7.48	Equipe com conhecimento técnico obsoleto	Pessoas	5.2.1 – Política de treinamento/atualização						

			5.2.4 – Incentivos à atualização profissional						
7.49	Não atendimento das demandas de TIC devido a férias da equipe	Pessoas	5.1.1 - Divisão clara de atribuições e responsabilidades						
7.50	Exclusividade na execução das tarefas de TIC	Pessoas	5.1.1 - Divisão clara de atribuições e responsabilidades						
7.51	Falta de apoio e resistência dos colaboradores durante o processo de desenvolvimento e implantação de software	Pessoas	5.1.4 - Integração entre setores						
7.52	Não envolver usuários-chave e usuário final no processo de desenvolvimento do <i>software</i>	Pessoas	5.1.4 - Integração entre setores						
7.53	Insatisfação devido a diferenças salariais e bonificações	Pessoas	5.1.5 - Remuneração						
7.54	Disputas internas da equipe de TIC	Pessoas	5.1.6 - Liderança e Gestão de Equipe						
7.55	Não alinhamento das estratégias de TIC com as estratégias do negócio (indefinição de estratégias, objetivos e metas de TIC)	Governança de TIC	6.1.2 - Determinação da Direção Tecnológica 6.1.3 - Definição de Processos de TI, Organização e Relacionamento. 6.1.5 – Comunicação de Metas e Diretivas Gerenciais 6.4.1 – Monitoramento e Avaliação da Performance de TIC 6.4.4 – Fornecimento da Governança de TIC						
7.56	Indisponibilidade de recursos financeiros para projetos de TIC	Governança de TIC	6.1.4 – Gerência do Investimento de TIC						
7.57	Interrupção ou má qualidade dos serviços prestados por parcerias estratégicas	Governança de TIC	6.2.6 – Gerenciamento do nível de serviços						
7.58	Recursos de TIC inadequados para atendimento dos serviços	Governança de TIC	6.2.7 – Gerenciamento de Capacidade						
7.59	Inadequada estrutura física da empresa	Governança de TIC	6.1.2 - Determinação da Direção Tecnológica						
7.60	Perda de competitividade por problemas tecnológicos	Governança de TIC	6.1.2 - Determinação da Direção Tecnológica						
7.61	Falha no mapeamento e desenho dos processos organizacionais	Governança de TIC	6.1.3 - Definição de Processos de TI, Organização e Relacionamento						
7.62	Falta de um plano de comunicação	Governança de TIC	6.1.5 - Comunicação de Metas e Diretivas Gerenciais						
7.63	Desastres naturais	Governança de TIC	6.1.7 - Avaliação e Gerência de Riscos						
7.64	Inatividade de fornecedores e parceiros estratégicos	Governança de TIC	6.2.11 - Gerenciamento de Fornecedor						
7.65	Dificuldade na alocação ou contratação de terceiros	Governança de TIC	6.2.11 - Gerenciamento de Fornecedor						
7.66	Treinamento dos usuários no uso do <i>software</i> e não nos processos	Governança de TIC	6.2.14 - Gerenciamento do Conhecimento						
7.67	Treinamento não qualificado	Governança de TIC	6.2.14 - Gerenciamento do Conhecimento						
7.68	Falta de documentação do software	Governança de	6.2.14 - Gerenciamento do						

		TIC	Conhecimento						
7.69	Elevação do custo do projeto de desenvolvimento e implantação do <i>software</i>	Governança de TIC	6.2.2 - Gerenciamento de Finanças						
7.70	Alterações das prioridades	Governança de TIC	6.2.4 - Gerenciamento de demanda						
7.71	Pressão para implantação de serviços e soluções de TIC	Governança de TIC	6.2.4 - Gerenciamento de demanda						
7.72	Elevação da carga horária dos colaboradores durante o processo de implantação do <i>software</i>	Governança de TIC	6.3.2 - Acompanhamento e Controle de Projeto						
7.73	Indefinição do cronograma de implantação e desenvolvimento do <i>software</i>	Governança de TIC	6.3.2 - Acompanhamento e Controle de Projeto						
7.74	Autuação devido a problemas de <i>software</i>	Governança de TIC	6.4.3 - Conformidade Regulatória						
7.75	Complexidade na legislação	Governança de TIC	6.4.3 - Conformidade Regulatória						
7.76	Falta de apoio da alta direção	Governança de TIC	6.4.4. - Fornecer Governança de TIC						

## APENDICE B – PLANO DE RESPOSTA AOS RISCOS DE TIC

ID	Riscos de TIC	Plano de Redução dos Riscos de TIC	Plano de Contingência dos Riscos de TIC	Custo para Redução (R\$)	Custo de Contingência (R\$)	Responsável	Prazo	Partes Interessadas	Status
7.1	Falha na instalação, configuração ou administração do Banco de Dados.	Utilizar pessoal capacitado Realizar validação antes da liberação Seguir as especificações técnicas	Identificar origem da falha Reinstalar ou reconfigurar o Banco de Dados						
7.2	Indisponibilidade do servidor (arquivos, banco de dados)	Realizar manutenções preventivas Monitorar funcionamento dos servidores	Verificar e corrigir funcionamento dos ativos de rede Verificar funcionamento do hardware Verificar regras de acesso						
7.3	Falta de capacidade e/ou redundância para armazenamento dos dados	Adquirir o hardware de acordo com projeção de crescimento do volume e dos serviços Monitorar volume dos dados Realizar manutenção preventiva	Liberar espaço Realizar backup e expurgo dos dados Adquirir dispositivos						
7.4	Política de backup inexistente ou inadequada	Implantar Política de backup	Atualizar processo e política de backup						
7.5	Indisponibilidade de mídias de backup	Programar aquisição de mídias de acordo com o volume de dados Controlar estoque das mídias	Adquirir mídias						
7.6	Acesso não autorizado às informações	Definir e implantar política de acesso dos usuários Monitorar acessos e tentativas de acessos dos usuários Realizar auditoria de segurança da informação Acompanhar movimentação do quadro de pessoal (demissão, contratação, realocação, etc.)	Bloquear acesso do usuário						
7.7	Espionagem industrial	Definir e implantar política de acesso dos usuários Monitorar acessos e tentativas de acessos dos usuários Realizar auditoria de segurança da informação Acompanhar movimentação do quadro de pessoal (demissão, contratação, realocação, etc.)	Bloquear acesso do usuário						

7.8	Vazamento ou perda de dados e informações	<i>Definir e implantar política de acesso dos usuários</i> <i>Monitorar acessos e tentativas de acessos dos usuários</i> <i>Realizar auditoria de segurança da informação</i> <i>Acompanhar movimentação do quadro de pessoal (demissão, contratação, realocação, etc.)</i> <i>Manter Política de backup</i>	<i>Bloquear acesso do usuário;</i> <i>Realizar backup dos dados</i>							
7.9	Perda de documentação e/ou código-fonte de softwares	<i>Manter política de backup</i> <i>Manter ou adquirir software para controle de versões</i>	<i>Manter ou adquirir software para controle de versões</i> <i>Realizar backup</i>							
7.10	Sabotagem no código-fonte	<i>Definir e implantar política de acesso dos usuários</i> <i>Monitorar acessos e tentativas de acessos dos usuários</i> <i>Realizar auditoria de segurança da informação</i>	<i>Verificar versões anteriores</i> <i>Corrigir e implantar nova versão do software</i>							
7.11	Falta de equipe capacitada para desenvolvimento das atividades	<i>Definir Matriz de Ação e Competência para cada função</i> <i>Recrutar e Selecionar seguindo as normas da organização</i> <i>Alocar os colaboradores nas funções de acordo com a competência de cada um</i> <i>Avaliar periodicamente o trabalho da equipe</i>	<i>Implantação de programa de treinamento e capacitação adequados ao negócio</i>							
7.12	Instalação e uso de softwares não licenciados	<i>Realizar frequentemente inventário</i> <i>Definir política de permissões de administrador do hardware</i> <i>Avaliar necessidades dos usuários</i> <i>Avaliar utilização de softwares livres ou licenciados</i>	<i>Desinstalação e remoção de softwares não licenciados</i> <i>Avaliar necessidade do software</i> <i>Avaliar possibilidade de adquirir software licenciado ou utilizar software livre</i>							
7.13	Indisponibilidade dos Sistemas, ERP, portais e sites.	<i>Monitorar ativos de rede</i> <i>Monitorar logs do banco de dados</i> <i>Acompanhar e analisar a frequência do registro de chamados e incidentes</i>	<i>Identificar origem do problema (servidor, ativos e estrutura de rede, banco de dados, internet e links de acesso)</i> <i>Acionar equipe técnica para correção do problema</i>							
7.14	Falha na definição ou indefinição das necessidades e prioridade dos usuários (requisitos não definidos claramente)	<i>Implantar PE de TIC</i> <i>Implantar metodologia para gerenciamento de requisitos</i> <i>Definir lista de tarefas e prioridades</i>	<i>Analisar requisitos da demanda</i> <i>Analisar e priorizar demandas dos usuários</i>							
7.15	Falha no desenvolvimento ou retrabalho devido a requisitos mal definidos	<i>Implantar metodologia adequada de projetos de desenvolvimento e</i>	<i>Redefinir requisitos</i> <i>Avaliar impacto das mudanças</i>							

		<i>manutenção de software</i>	<i>Definir prazos</i>						
7.16	Testes e homologações mal realizados	<i>Definir claramente requisitos Disponibilizar ambiente para usuário homologar as tarefas</i>	<i>Analisar requisitos Corrigir problemas</i>						
7.17	Falha na implantação	<i>Disponibilizar ambiente de desenvolvimento Disponibilizar ambiente de homologação para simulação e validação das implantações Utilizar software para controle de versões</i>	<i>Retornar versão funcional Avaliar e corrigir falhas</i>						
7.18	Não aquisição de licenças associadas ao novo software	<i>Identificar volumes e tipos de licenças necessárias a um novo software adquirido Realizar aquisição de licenças necessárias</i>	<i>Realizar aquisição de licenças necessárias</i>						
7.19	Falhas no processo de migração de dados	<i>Identificar processos e requisitos dos dados a serem migrados Realizar testes e homologações com o usuário Criar mecanismos de validação dos dados migrados</i>	<i>Identificar processos e requisitos inválidos Corrigir processo de migração Validar junto ao usuários</i>						
7.20	Não migração dos sistemas legados	<i>Manter equipe com conhecimento técnico do sistema Manter documentação Criar base de conhecimento sobre o sistema Manter backup dos dados e dos sistemas</i>	<i>Manter equipe com conhecimento técnico do sistema Manter documentação Criar base de conhecimento sobre o sistema Manter backup dos dados e dos sistemas</i>						
7.21	Indisponibilidade de serviços bancários <i>on line</i> (versão do java)	<i>Criar ambiente para testes e validações de novas versões Mapear impacto da atualização em outros softwares e serviços de TIC Manter backup das versões</i>	<i>Retornar versão anterior</i>						
7.22	Aquisição de <i>software</i> inadequado ao processo do negócio	<i>Envolver todos os usuários relacionados ao processo Mapear processos e regras de negócios Analisar aderência do software ao processo Avaliar softwares similares Avaliar fornecedor</i>	<i>Verificar possibilidade de desfazer a aquisição Verificar se processo pode ser melhorado</i>						
7.23	Falha de integração dos novos <i>softwares</i> com sistemas legados								
7.24	Alterações nos processos, requisitos e regras de negócio durante o desenvolvimento do	<i>Manter comunicação entre as áreas</i>	<i>Reavaliar processos, requisitos e regras de negócio.</i>						

	<i>software.</i>	<i>Mapear corretamente os processos Envolver usuários</i>	<i>Avaliar impacto das mudanças Rever cronograma e custos</i>						
7.25	<i>Software desenvolvido não atende às exigências dos processos organizacionais</i>	<i>Envolver todos os usuários relacionados ao processo Mapear processos e regras de negócios Analisar aderência do software ao processo Usuário realizar testes e homologações</i>	<i>Reavaliar processos, requisitos e regras de negócio. Avaliar impacto das mudanças Rever cronograma e custos</i>						
7.26	<i>Falha no processo de testes e homologação do software</i>	<i>Realizar testes e homologações</i>	<i>Corrigir problemas Realizar testes e homologações Implantar nova versão</i>						
7.27	<i>Falta de manutenção de hardware</i>	<i>Mapear hardware e serviços críticos Adquirir hardware de backup/redundância Avaliar utilização de serviços em nuvem Criar imagem do hardware</i>	<i>Recuperar o hardware ou implantar serviço em outro hardware</i>						
7.28	<i>Falta de hardware de backup para serviços críticos</i>	<i>Implantação de site backup Migrar serviços estratégicos para nuvem Distribuir serviços em localidades diferentes Manter mídias de backup em locais distintos</i>	<i>Reativar serviços que possuem contingência/redundância</i>						
7.29	<i>Não continuidade dos serviços de TIC após desastres (naturais, vandalismo, incêndios, etc)</i>	<i>Instalar e manter nobreak Instalar rede elétrica redundante</i>	<i>Executar procedimentos de desligamento dos equipamentos</i>						
7.30	<i>Falta de energia</i>	<i>Formar equipe de acordo com as necessidades do negócio Capacitar a equipe Alocar pessoas em atividades conforme a experiência e conhecimento Compartilhar conhecimentos Envolver a equipe nas tarefas</i>	<i>Capacitar a equipe</i>						
7.31	<i>Falta de experiência da equipe de desenvolvimento TIC</i>	<i>Avaliar fornecedor Verificar prazo e condições de transporte Antecipar a compra</i>	<i>Verificar a existência de hardware redundante Verificar possibilidade de transporte próprio</i>						
7.32	<i>Atraso na entrega do hardware</i>	<i>Avaliar todos os requisitos do software Avaliar ativos de rede e servidores da empresa</i>	<i>Redimensionar hardware Verificar a possibilidade de deslocamento ou transferência de recursos de software</i>						



		<i>Não implantar antes de um projeto piloto e paralelo</i>	<i>Verificar possibilidade de Cloud Computing</i>						
7.33	Dimensionamento inadequado do hardware para novo software	<i>Monitorar uso de rede, servidores e recursos Realizar manutenções preventivas Manter o parque de TI atualizado</i>	<i>Identificar “gargalos” Redimensionar hardware Verificar a possibilidade de deslocamento ou transferência de recursos de software Verificar possibilidade de Cloud Computing</i>						
7.34	Sobrecarga da rede e servidores	<i>Avaliar Central Telefônica redundante Verificar disponibilidade de serviço em nuvem Implantar linhas diretas em setores estratégicos Manter contrato de manutenção da Central</i>	<i>Ativar Central Telefônica redundante Acionar fornecedor para manutenção</i>						
7.35	Indisponibilidade da Central Telefônica	<i>Utilizar serviços de mais de uma operadora</i>	<i>Acionar operadora Utilizar serviço de telefonia fixa</i>						
7.36	Indisponibilidade do Serviço de Telefonia Móvel	<i>Utilizar serviços de telefonia móvel</i>	<i>Acionar operadora Utilizar serviço de telefonia móvel</i>						
7.37	Indisponibilidade do Serviço de Telefonia Fixa	<i>Monitorar usuários que tem acesso ao uso do e-mail corporativo Criar política de educação quanto ao uso do e-mail Implantar Política de Segurança da Informação</i>	<i>Orientar o colaborador quanto ao correto uso do e-mail</i>						
7.38	Uso indevido do e-mail	<i>Rever frequentemente permissões e acessos dos usuários Analisar logs de acesso Implantar Política de Segurança da Informação</i>	<i>Remover permissões de acesso do usuário</i>						
7.39	Acesso indevido ou não autorizado à rede, ativos e recursos de TIC.	<i>Manter rede estruturada Monitorar utilização da rede Realizar manutenção preventiva Manter redundância dos principais ativos e links</i>	<i>Identificar origem e corrigir problema</i>						
7.40	Indisponibilidade da rede física	<i>Manter rede estruturada Monitorar utilização da rede Realizar manutenção preventiva Manter redundância dos principais ativos</i>	<i>Identificar origem e corrigir problema</i>						
7.41	Indisponibilidade da rede sem fio	<i>Implantar e manter atualizado controle de acesso e permissões dos usuários Implantar sistema de</i>	<i>Remover acessos do usuário</i>						

		<i>monitoramento dos acessos</i> <i>Analisar logs de acesso</i> <i>Criar e implantar política de segurança da informação</i>							
7.42	Acesso ou uso indevido da internet	<i>Realizar auditoria de segurança da informação</i> <i>Manter a política de segurança da informação atualizada</i> <i>Aquisição e manutenção de antivírus</i> <i>Monitorar permissões de acesso dos usuários</i>	<i>Identificar e remover ameaça</i> <i>Atualizar antivírus</i> <i>Rever regras de segurança</i>						
7.43	Vulnerabilidade quanto a ataques externos ou softwares maliciosos	<i>Monitorar frequentemente o link de internet</i> <i>Manter link de contingência</i> <i>Manter calendário de testes do link de contingência</i>	<i>Ativar link de contingência</i>						
7.44	Indisponibilidade do serviço ou link de internet								
7.45	Vulnerabilidade do antivírus e/ou firewall	<i>Definir claramente necessidades e competências das funções</i> <i>Contratação rigorosa</i>	<i>Promover treinamento e capacitação do pessoal</i> <i>Contratar pessoas qualificadas</i>						
7.46	Contratação de pessoal não qualificado ou apto para desenvolvimento das funções	<i>Promover pesquisa de satisfação</i> <i>Definir claramente as responsabilidades</i> <i>Envolver a equipe nas decisões da área</i> <i>Criar projetos desafiadores</i> <i>Promover capacitação e atualização tecnológica</i> <i>Promover o reconhecimento e valorização do trabalho</i> <i>Descentralizar o trabalho e socializar o conhecimento</i>	<i>Avaliar clima organizacional</i> <i>Executar programa de incentivo</i>						
7.47	Desmotivação da equipe de TIC e/ou perda de talentos	<i>Implantar política de treinamento e capacitação</i> <i>Incentivar atualização profissional</i>	<i>Promover treinamento e capacitação do pessoal</i>						
7.48	Equipe com conhecimento técnico obsoleto	<i>Manter calendário e/ou programação de férias</i> <i>Procurar adequar prazos à disponibilidade da equipe</i>	<i>Verificar possibilidade de suspender as férias</i> <i>Verificar possibilidade de contratação de terceiros</i> <i>Negociar prazos</i>						
7.49	Não atendimento das demandas de TIC devido a férias da equipe	<i>Definir claramente os papéis e responsabilidade de cada um</i> <i>Não concentrar os trabalhos em um único colaborador</i> <i>Procurar ter sempre</i>	<i>Promover rodízio de tarefas</i>						

		<i>colaboradores “backup” Promover rodízio de tarefas Manter base de conhecimento</i>							
7.50	Exclusividade na execução das tarefas de TIC	<i>Implantar política de comunicação e transparência Conciliar as tarefas dos usuários no processo de desenvolvimento e implantação com a rotina Orientar e esclarecer necessidade e importância do software</i>	<i>Implantar política de comunicação e transparência Conciliar as tarefas dos usuários no processo de desenvolvimento e implantação com a rotina Orientar e esclarecer necessidade e importância do software</i>						
7.51	Falta de apoio e resistência dos colaboradores durante o processo de desenvolvimento e implantação de software	<i>Identificar quais os usuários chave e finais de cada processo de negócio Realizar reuniões frequentes</i>	<i>Identificar quais os usuários chave e finais de cada processo de negócio Realizar reuniões frequentes</i>						
7.52	Não envolver usuários-chave e usuário final no processo de desenvolvimento do software	<i>Identificar e comunicar papéis e responsabilidade de cada um Implantar plano de cargos e salários</i>	<i>Implantar plano de cargos e salários</i>						
7.53	Insatisfação devido a diferenças salariais e bonificações	<i>Realizar reuniões frequentes com a equipe Identificar conflitos Definir papéis e responsabilidades Avaliações periódicas</i>	<i>Identificar causas dos conflitos Definir plano de atuação</i>						
7.54	Disputas internas da equipe de TIC	<i>Realizar e manter o PE de TIC Criar plano de Comunicação e Transparência de TIC</i>	<i>Alinhar os projetos de TIC de acordo com os objetivos estratégicos da organização Redefinir prioridades</i>						
7.55	Não alinhamento das estratégias de TIC com as estratégias do negócio (indefinição de estratégias, objetivos e metas de TIC)	<i>Promover o orçamento anual de TIC Buscar fornecedores e parcerias alternativas Avaliar utilização de plataformas open-source</i>	<i>Reavaliar projetos e prioridades Desenvolver novos fornecedores e serviços</i>						
7.56	Indisponibilidade de recursos financeiros para projetos de TIC	<i>Avaliar e qualificar os serviços dos parceiros Desenvolver fornecedores alternativos Atentar para a formalização e questões contratuais</i>	<i>Executar as medidas contratuais cabíveis Procurar novos fornecedores ou parceiros</i>						
7.57	Interrupção ou má qualidade dos serviços prestados por parcerias estratégicas	<i>Mapear processos e Serviços de TIC Manter PE de TIC</i>	<i>Definir prioridades junto às áreas Adquirir recursos que atendam as necessidades</i>						
7.58	Recursos de TIC inadequados para atendimento dos serviços	<i>Avaliar estrutura de TIC da empresa Montar plano de adequação da</i>	<i>Montar plano de adequação da TIC às necessidades do negócio Definir prioridades e</i>						

		<i>TIC às necessidades do negócio</i> <i>Definir prioridades e orçamento</i>	<i>orçamento</i>						
7.59	Inadequada estrutura física da empresa	<i>Manter parque de TI atualizado</i> <i>Implantar Gestão de Serviços</i>	<i>Reavaliar e estrutura e serviços de TIC</i>						
7.60	Perda de competitividade por problemas tecnológicos	<i>Implantar cultura de processos</i> <i>Manter equipe capacitada</i> <i>Manter processos revisados e atualizados</i>	<i>Atualizar processos</i>						
7.61	Falha no mapeamento e desenho dos processos organizacionais	<i>Montar Plano de Comunicação e Transparência de TIC</i>	<i>Montar Plano de Comunicação e Transparência de TIC</i>						
7.62	Falta de um plano de comunicação	<i>Avaliar e qualificar fornecedores</i> <i>Manter alternativas aos serviços executados por fornecedores</i>	<i>Pesquisar fornecedores substitutos ou executar serviço internamente</i>						
7.63	Desastres naturais	<i>Identificar no mercado potenciais fornecedores de serviços</i> <i>Formar e capacitar equipe interna</i>	<i>Identificar no mercado potenciais fornecedores de serviços</i> <i>Formar e capacitar equipe interna</i>						
7.64	Inatividade de fornecedores e parceiros estratégicos	<i>Separar atividades de processo e de software</i> <i>Definir como objetivo do treinamento o processo</i> <i>Disseminar a ideia de que o software é uma ferramenta de apoio ao processo</i>	<i>Capacitar os usuários no processo</i>						
7.65	Dificuldade na alocação ou contratação de terceiros	<i>Realizar treinamentos aderentes ao negócio</i> <i>Identificar fornecedores qualificados</i> <i>Manter registro e avaliação dos treinamentos</i>	<i>Rever Levantamento da Necessidade de Treinamento</i>						
7.66	Treinamento dos usuários no uso do <i>software</i> e não nos processos	<i>Exigir registro da documentação do software</i> <i>Manter base de conhecimento</i> <i>Realizar backup da documentação</i>	<i>Promover a documentação do software</i>						
7.67	Treinamento não qualificado	<i>Definir as entregas</i> <i>Cumprir os prazos</i> <i>Dimensionar a equipe</i>	<i>Redefinir prioridades</i>						
7.68	Falta de documentação do software	<i>Definir prioridades</i> <i>Estabelecer acordos de entrega</i> <i>Cumprir prazos</i>	<i>Redefinir prioridades</i> <i>Avaliar impacto</i>						
7.60	Elevação do custo do projeto de desenvolvimento e implantação do <i>software</i>	<i>Implantar cultura de projetos</i> <i>Acompanhar e monitorar a execução das tarefas</i> <i>Atualizar cronograma</i> <i>Dimensionar a equipe conforme a</i>	<i>Redefinir prioridades e entregas</i> <i>Verificar possibilidade de contratação de pessoal</i>						

		<i>necessidade</i>							
7.70	Alterações das prioridades	<i>Implantar cultura de projetos Definir entregas</i>	<i>Identificar status do projeto Redefinir prioridades Redefinir prazos</i>						
7.71	Pressão para implantação de serviços e soluções de TIC	<i>Desenvolver software em conformidade com a legislação Manter regras de negócio e requisitos atualizados Contratar consultoria especializada</i>	<i>Contratar consultoria especializada Atualizar software de acordo com a conformidade</i>						
7.72	Elevação da carga horária dos colaboradores durante o processo de implantação do software	<i>Contratar consultoria especializada</i>	<i>Contratar consultoria especializada</i>						
7.73	Indefinição do cronograma de implantação e desenvolvimento do software	<i>Manter Plano de Comunicação e Transparência Divulgar informações sobre a TIC Cumprir os prazos acordados Manter os serviços de TIC disponíveis</i>	<i>Manter Plano de Comunicação e Transparência Divulgar informações sobre a TIC</i>						
7.74	Autuação devido a problemas de software	<i>Mapear e comunicar responsabilidades e papéis</i>	<i>Definir e comunicar papéis e responsabilidades</i>						
7.75	Complexidade na legislação	<i>Manter Plano de Comunicação e Transparência Divulgar informações sobre a TIC Realizar workshop de serviços de TIC</i>	<i>Manter Plano de Comunicação e Transparência Divulgar informações sobre a TIC Realizar workshop de serviços de TIC</i>						
76	Falta de apoio da alta direção	<i>Manter Plano de Comunicação e Transparência Cumprir prazos das entregas</i>	<i>Manter Plano de Comunicação e Transparência Cumprir prazos das entregas</i>						

## APENDICE C – PLANO DE COMUNICAÇÃO E TRANSPARÊNCIA DE TIC

ID	Informação	Classificação	Responsável	Formato ou Layout	Destinatários	Meio de Comunicação	Periodicidade	Vigência	Descarte / Arquivamento
8.1	Resultados periódicos dos indicadores de TIC								
8.2	Interrupção ou indisponibilidade dos Serviços de TIC								
8.3	Catálogo de Produtos e Serviços de TIC								
8.4	Divulgação dos Projetos de TIC								
8.5	Divulgação missão, visão, objetivos e metas de TIC								
8.6	Comunicação sobre ocorrência dos riscos catalogados								
8.7	Orientação quanto ao uso dos recursos de TIC								
8.8	Política de Segurança da Informação								
8.9	Notificação do uso indevido dos recursos de TIC								
8.10	Notificação das alterações e manutenções nos <i>softwares</i> , sistemas ou ERP.								
8.11	Informação sobre a aplicação dos recursos financeiros na área de TIC								
8.12	Notificação sobre contratações e desligamentos de componentes da equipe de TIC								
8.13	Comunicação de alterações em prazos e prioridades acordados com os usuários								
8.14	Papéis e responsabilidades do pessoal de TIC								
8.15	Escala de trabalho da equipe de TIC								

## APENDICE D – CRITÉRIOS DE PRIORIZAÇÃO DOS PROCESSOS DE TIC

Critério	Peso	Valores (de 0 a 4)
ROI	10	0 – Muito Baixo / 1 – Baixo / 2 – Médio / 3 – Alto / 4 – Muito Alto.
Exigência de Norma / Lei	10	0 – Não previsto em lei, resolução ou norma interna / 1, 2 - Previsto em lei sem prazo / 3 – Previsto em lei, resolução ou norma interna com prazo que não exige início imediato observado o esforço necessário para sua realização / 4 – (DETERMINANTE) Previsto em lei, resolução ou norma interna com prazo que exige início imediato observado o esforço necessário para sua realização.
Evita Colapso na infraestrutura	10	0 – Não / 1 – Sim. Com baixo impacto / 2 – Sim. Com médio impacto / 3 – Sim. Com alto impacto / 4 – (DETERMINANTE) Sim. Com impacto muito alto.
Alinhamento Estratégico	9	0 - Não atende nenhuma ação / 1 – Atende parcialmente a uma ação estratégica / 2 – Atende parcialmente a duas ações / 3 – Atende mais de duas ações parcialmente / 4 – Corresponde exatamente a uma ação estratégica.
Principais stakeholders beneficiados	7	1 – Atende até 50% dos clientes internos / 2 – Atende até 70% dos clientes internos / 3 – Atende a mais de 70% dos clientes internos / 4 – Atende a clientes internos e externos.
Custo	6	0 – Superior a 60% do recurso orçamentário respectivo / 1 - Até 60% do recurso orçamentário respectivo / 2 – Até 40% do recurso orçamentário respectivo / 3 - Até 30% do recurso orçamentário respectivo / 4 – Sem custo de aquisição / contratação.
Riscos	5	0 – Muito Alto / 1 – Alto / 2 – Médio / 3 – Baixo / 4 – Muito baixo
Probabilidade de entrega	5	0 – Muito Baixa / 1 – Baixa / 2 – Média / 3 – Alta / 4 – Muito Alta.
Esforço	6	0 – Acima de 2500 homens/hora / 1 – 2001 até 2500 homens/hora. / 2 – 1501 até 2000 homens/hora / 3 - 1001 até 1500 homens/hora. / 4 – Até 1000 homens/hora.
Otimização de recursos	5	0 – Não há redução de recursos / 1 – Reduz recursos materiais / 2 – Reduz tempo / 3 – Reduz recursos humanos / 4 – Reduz recursos humanos além de recursos materiais ou tempo.